

CRB



CALIFORNIA
STATE LIBRARY
FOUNDED 1850

California Research Bureau

900 N Street, Suite 300
P.O. Box 942837
Sacramento, CA 94237-0001
(916) 653-7843 phone
(916) 654-5829 fax

Security and Privacy Recommendations for Government Issued Identity Documents Using Radio Frequency Identification Tags or Other Technologies

By Chris J. Marxen

*Prepared at the Request of
Senator S. Joseph Simitian*

MAY 2008

CRB 08-008

C A L I F O R N I A R E S E A R C H B U R E A U

Security and Privacy
Recommendations for
Government-Issued Identity
Documents Using Radio
Frequency Identification Tags
or Other Technologies

By Christopher J. Marxen

*Prepared at the Request of
Senator S. Joseph Simitian*

ISBN 1-58703-238-4

Acknowledgments

The author of this report would like to thank Pam Martin and Pamela Rasada for their assistance organizing data received during the process of obtaining information for this report and Amy Sullivan for her assistance organizing the public meetings.

Special thanks to Jan Boel, formerly of the Governor's Office of Planning and Research and the Public Employee Post-Employment Benefits Commission, for her direction and guidance.

**Request for Report
From California State Senator
S. Joseph Simitian**

CAPITOL OFFICE
STATE CAPITOL, ROOM 4062
SACRAMENTO, CA 95814
TEL (916) 651-4011
FAX (916) 323-4529
SENATOR.SIMITIAN@SEN.CA.GOV
WWW.SEN.CA.GOV/SIMITIAN

California State Senate

**SENATOR
S. JOSEPH SIMITIAN
ELEVENTH SENATE DISTRICT**



DISTRICT OFFICE
160 TOWN & COUNTRY VILLAGE
PALO ALTO, CA 94301
TEL (650) 688-6384
FAX (650) 688-6370

SATELLITE OFFICE
701 OCEAN ST., ROOM 318-A
SANTA CRUZ, CA 95060
TEL (831) 425-0401
FAX (831) 425-5124

October 4, 2007

Mr. Dean Mischynski
California Research Bureau
900 N Street, Suite 300
Sacramento, CA 95814

Dear Mr. Mischynski:

As you know, the right to privacy is a personal and fundamental right protected by the California Constitution. As such, all Californians have an inherent right to privacy with regard to the distribution, storage, and use of their personal information by government.

In order to ensure that the State of California maintains stringent privacy standards, while exploring the potential benefits of new electronic identification technologies, state policymakers need a continuous supply of good data about how best to secure personal privacy in an age of ubiquitous computing. To that end, I ask the California Research Bureau (CRB) to prepare and deliver a report on security and privacy recommendations for government-issued, radio frequency identification (RFID)-enabled identity documents (IDs).

I would also like to request that the CRB establish an advisory board to provide technical support, answer bureau questions, outline the strengths and weaknesses of potential approaches to privacy and security protocols, and assist the CRB in the completion of the report.

Sincerely,

A handwritten signature in blue ink, appearing to read "Joe Simitian".

S. Joseph Simitian
State Senator, 11th District



Table of Contents

EXECUTIVE SUMMARY	1
THE RADIO-FREQUENCY IDENTIFICATION DOCUMENT ADVISORY PANEL	11
JUSTIFICATION FOR SUBMITTED RECOMMENDATIONS	14
RECOMMENDATIONS.....	18
APPENDIX A: TEXT OF SENATE BILL 30 (2007).....	36
APPENDIX B: RADIO-FREQUENCY IDENTIFICATION DOCUMENT ADVISORY PANEL COMMENTS.....	49
APPENDIX C: SAM FEASABILITY STUDY	54
APPENDIX D: PRIVACY PROVISIONS FROM THE E-GOVERNMENT ACT OF 2002	60
APPENDIX E: OFFICE OF MANAGEMENT AND BUDGET E-GOVERNMENT ACT SECTION 208 IMPLEMENTATION GUIDANCE	64
APPENDIX F: PUBLIC PARTICIPATION PROVISIONS OF THE ADMINISTRATIVE PROCEDURES ACT (GOVERNMENT CODE SECTIONS 11346-11348)	83
APPENDIX G: STATE ADMINISTRATIVE MANUAL SECTION 4841.2 (INFORMATION INTEGRITY AND SECURITY)	99

Executive Summary

Recommendations For New Government Issued Identification Documents

This report presents recommendations to the California State Legislature regarding issues identified by the California Research Bureau (CRB) regarding the selection and use of new or substantially modified government issued identification documents. The recommendations were developed in consultation with the Radio-Frequency Identification Document Advisory Panel that

was established pursuant to a request from Senator S. Joseph Simitian. (In 2007, Senator Simitian authored a legislative bill on the subject (SB 30) which is contained in Appendix A.) The following recommendations are divided into eight groups which together constitute a plan for addressing issues associated with the documents.

Group 1 Applicability and Exemptions

Recommendation 1

Applicability to K-12 Schools:

It is recommended that the applicability of the state information management principles in this report or contained in Chapter 4800, et seq. (Information Technology) of the State Administrative Manual (SAM) be extended to K-12 public schools as defined in Sections 50-53 of the Education Code. This includes public schools and schools only partly supported by the State, including day and evening elementary and secondary schools.

It is further recommended that the information electronically transmitted from an identification document issued to a California public school K-12 student be limited to the Statewide Student Identifier number issued pursuant to the provisions of Section 49084(e)(3) of the Education Code.

Recommendation 2

Applicability to State Agencies Currently Exempted from State Information Management Principles:

It is recommended that the applicability of the State information management principles in this report or contained in Chapter 4800 et. seq. of the State Administrative Manual be extended to certain state entities currently exempted by Section 4810 of SAM. These include the University of California, the California State University, community college districts, and the Legislature.

Executive Summary

Group 2
Need,
Technology and
Privacy
Assessment

Recommendation 3

Applicability to Local Agencies:

These recommendations should apply to all “local agencies” when they implement a new government-issued identification system or when they make changes to identification documents or related systems that may create new privacy risks. “Local agencies” are defined in California Government Code Section 6252 and include counties, cities (whether general law or chartered), cities and counties, school districts, and special districts.

Recommendation 4

Exemption for Agencies:

Agencies should be able to choose to implement new identification systems or modify existing systems without meeting these recommendations where the identification system is only used for internal government operations (when there is no requirement for a member of the general public to obtain or use the identification document) or has been previously assessed under an evaluation similar to that contained in Recommendation 10.

Recommendation 5

Local government agencies should identify information technology needs during a feasibility study process. As part of the process, the feasibility study should contain the following provisions:

- An analysis of the problem (or opportunity) in terms of its effect on the agency’s mission and programs;
- An analysis of the strengths or weaknesses of any existing identification document used by the agency;
- An identification of the organization’s managerial and technical environment within which a response to the problem or opportunity will be implemented;
- Clearly established programmatic and administrative objectives, and;
- Concise functional requirements.

Recommendation 6

All State agencies should consider a range of feasible form factors or features for a new identification document appropriate to the data privacy and security needs of the system in the technology assessment portion of the feasibility study required by Chapter 4900 of SAM. Depending on the functional requirements of the system, the identification document may

include, but is not necessarily limited to, the following form factors or features:

- Radio Frequency (RF) Technologies;
- Color Shifting Ink;
- Holograms;
- Microprinting;
- UV Sensitive Printing;
- Magnetic Strips;
- Smart Cards;
- Bar Codes (linear and 2D);
- Watermarks;
- Security Threads;
- Guilloche printing;
- Color Printing, and/or;
- Serial Numbers.

Recommendation 7

All State agencies should conduct a privacy impact assessment in the technology assessment portion of the feasibility study required by Chapter 4900 of SAM. In order to assess the impact of the system design upon the data privacy of intended users of the identification document, the privacy impact assessment may include, but not necessarily be limited to:

- What information will be physically or electronically stored or printed on the document;
- What information will be collected and/or stored in the data management system;
- Rationale for the storage and/or printing of the information on the document;
- Why the information is being read, collected, and/or stored by the issuer;
- The intended use of the information;
- With whom the information will be shared (e.g., another agency for a specified purpose);
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information and how individuals can grant consent, and;
- How the information will be secured (e.g., administrative and technological controls) both in the data management system and on the document itself.

Executive Summary

Recommendation 8

To assess the impact of the system upon the data privacy of intended users of the identification document, all State agencies should conduct a privacy impact assessment as part of the feasibility study required by Chapter 4900 of SAM. This analysis should include:

- An identification of what choices the agency made regarding the new or modified government-issued identification document system as a result of performing the privacy impact assessment;
- A privacy impact analysis related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, an initial risk assessment;
- An analysis of the impact the system will have on an individual's data privacy, specifically identifying and evaluating potential threats to the extent these elements are known at the initial stages of development, and;
- The privacy impact assessment may need to be updated before deploying the system to consider elements not identified at the concept stage, or to address choices made in designing the system unknown at the time of the initial assessment

Recommendation 9

All State agencies should include an analysis of the following security risks in the feasibility study required by Chapter 4900 of SAM:

- An analysis of the security risks of any known identification document attacks or vulnerabilities and the technologies that counteract those attacks or vulnerabilities. These include, but are not necessarily limited to, the following:
 - Vulnerability of the identification document to cloning;
 - Vulnerability of the identification document to tampering;
 - Vulnerability of the identification document to skimming (using an unauthorized reader to obtain information from the document);
 - Ability to read the data stored on the identification document either legitimately or illegitimately without user knowledge;
 - Vulnerability of the identification document to counterfeiting;
 - Vulnerability of the identification document to spoofing (utilizing a device or devices to transmit electronic data as if it were coming from the actual document);

Executive Summary

- Read range (how far away the document can electronically transmit data);
- Vulnerability of the identification document to tracking (the ability to follow a person carrying the document utilizing electronic data being transmitted by the document), and/or;
- Vulnerability of the identification document to replay and relay attacks. [In a “replay” attack, an unauthorized person broadcasts an exact re-transmission of a previous legitimate transmission made from a user’s card. In a “relay” attack, (otherwise known as a “man in the middle” attack), an unauthorized person receives signals broadcast between a legitimate card and reader and sends those signals to an offsite location to complete an unauthorized transaction].
- An analysis of the necessity of features to ensure adequate defense against security risks not limited to those listed previously, including, but not limited to:
 - Encryption of the data stored on the document;
 - Basic Access Controls, such as the use of a Personal Identification Number (PIN);
 - Authentication between the document and an electronic reader;
 - Radio frequency shielding devices in the event that radio frequency technologies are integrated into the document;
 - On/off switches, and;
 - Opt out/in options.

Recommendation 10

Local agencies should include the provisions contained in Recommendations 6 through 9 in their feasibility study.

Group 3

Public Education and Security and Privacy Protections

Recommendation 11

When deploying a new government identification document or system, State and local government agencies should enact rules to ensure that the user’s data privacy is protected to the maximum practical extent if the document is reported to be lost or stolen, and should provide the user with information on how to protect security when the document is discarded. The agency should also provide information to holders of new or modified identification documents regarding how the system works and how personal data, if any, will be used or managed:

Executive Summary

- The reason that the identification document was issued should be provided;
- The public should be notified which personal information, if any, is stored electronically in the document or is being collected, transmitted, or stored elsewhere;
- The agency should provide a clear description of the privacy or security risks that may be associated with the identification document, and advise on how the user can minimize these risks and an explanation of any rights the user may have to opt out of using the identification document, to restrict the amount of information on the document or to limit its readability, or to otherwise reduce any privacy or security risks associated with its use. Both the risks and the instructions for minimizing risks should be presented in language that a non-technical person can comprehend;
- The agency should maintain a telephone contact number or email address or web site for questions;
- When a document is lost or stolen, the agency should have a process in place to minimize the potential for unauthorized use of the document and to limit access to personal information that may be contained within the document, and;
- Agencies should develop procedures for the public to follow to protect the user's privacy and security when disposing of the identification document. These may include, but are not limited to, procedures to deactivate, destroy, or otherwise render the document unreadable or unusable. Members of the public should receive a copy of these procedures when they first get their identification document, and the procedures should be posted on web sites and otherwise accessible later, when they actually need them.

Group 4 Public Participation

Recommendation 12

State and local government agencies should involve the public in discussions regarding the adequacy of the privacy impact assessment:

- Agencies should publish and distribute a public notice of the proposed privacy impact assessment and a statement of the time, place, and nature of a public hearing. In addition to the general public notice, agencies should attempt to identify and provide notice to groups and individuals with an interest in privacy and technology issues;

- At the public hearing, both oral and written statements should be permitted;
- The agency should consider any comments received and make changes to the privacy impact assessment as warranted;
- The agency should prepare a draft “privacy and security determination statement” summarizing each objection or recommendation regarding the specific amendment proposed together with an explanation of how the final privacy impact assessment has been changed to accommodate each objection or recommendation, or the reasons for making no change. The statement should also contain a written determination that no alternative considered by the agency would be more effective in carrying out the objectives of the new or modified system, and;
- The draft determination statement should be posted and publically noticed by the agency at least 30 days before the agency makes a final determination statement.

Recommendation 13

Public notice for the hearing on the proposed privacy impact assessment should be filed with the California Office of Information Security and Privacy Protection, which should distribute the notice to parties it believes to be interested.

Recommendation 14

The draft determination statement shall also be filed with the California Office of Information Security and Privacy Protection.

Group 5 Public Access to Records and Administrative Remedies

Recommendation 15

It is recommended that Article 8 of the Information Practices Act of 1977 (California Civil Code Sections 1798.30-1798.44) be amended to include local government agencies and the Legislature. The Information Practices Act gives holders of government-issued identification documents the right to inquire as to whether the agency maintains a record about himself or herself and to make those records available. The Act also provides administrative remedies.

Recommendation 16

It should be the policy of State and local government agencies not to read identification documents without the knowledge of their holders. At

Executive Summary

locations where a State or local government agency intends to read identification documents that are so sufficiently remote that the identification document holder might be unaware, the agency should alert the user to the location of any devices used by the agency to read the data on the identification document. This recommendation may be satisfied by one or more of the following:

- Posting or displaying a clear and conspicuous sign, placard, poster, or other similar notice at each reader's actual location indicating that the issuing authority has placed an identification document reader at that location, that the reader is being used to read identification documents remotely, and the commonly understood name of each document. The notice might be in the form of a written statement, or it might consist of a widely publicized symbol for an identification document reader;
- Providing each document holder with a list of the location of all readers used or intended to be used by the issuing authority to read the data on the identification document, and/or;
- Providing each document holder with a direct Internet link to a web page that clearly and conspicuously lists the location of all readers used or intended to be used by the issuing authority to read the data on the identification document. This web page shall be kept up to date.

Recommendation 16 will not apply in those instances where the release of a reader's location will pose a security risk to property, if it will increase the likelihood that confidential information will be released, or if the release of the location endangers human life or safety.

Group 6 Public Feedback

Recommendation 17

A state or local government agency should provide the opportunity for the public to offer feedback to the agency about its identification document or system. This should include:

- Providing users a method to comment on the system both prior to and after deployment;
- Providing users a method to report unauthorized use, abuse, or fraud, and;
- The agency should conduct an occasional survey of users after deployment in order to understand any issues or concerns by document users.

Group 7

Proactive Response to Breach

Recommendation 18

It is recommended that California Civil Code Section 1798.3(b) (definition of “Agency”) be amended to include local government agencies. This change would make local government agencies subject to California Civil Code Section 1798.29 that requires agencies owning or licensing computerized data containing personal information to disclose any breach of the system’s security to a California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Recommendation 19

A state or local government agency that experiences a breach in its government-issued identification document system should take action to eliminate or substantially reduce the probability of a similar breach occurring within 90 days of the date that the breach occurred.

Group 8

Data Management and Access

Recommendation 20

For all databases containing information from government-issued identification documents, local government agencies should :

- Identify all automated files and databases for which the agency has ownership responsibility;
- Ensure that responsibility for each automated file or database is defined
- Enter into agreements with non-State entities that have access to confidential information received from the identification document for security, and;
- Establish appropriate policies and procedures to protect and secure information technology infrastructure.

Group 9

Penalties for Noncompliance

Recommendation 21

California Penal Code Section 502 is the core definition of “computer crimes” in California law. It is recommended that this section be amended to include government issued identification documents containing electronic data as an input device for “computer systems”.

Recommendation 22

It is recommended that California Penal Code Section 502(c) be amended to include the theft, interference with, or unauthorized access to data from

Executive Summary

government-issued identification documents containing electronic data as a specific public offense.

Recommendation 23

It is recommended that California Penal Code Section 502(d)(1) be amended to include the public offense noted in Recommendation 22 as a crime punishable by up to 2-3 years of prison and a \$10,000 fine.

Recommendation 24

It is recommended that California Penal Code Section 502.6(a) (fraudulent use of information from magnetic stripe credit and debit cards) be amended to include all government-issued identification technologies utilizing electronically-coded personal data.

Recommendation 25

It is recommended that California Civil Code Section 1798.90.1 (drivers license data contained on magnetic stripe) be amended to include all government-issued identification technologies utilizing electronically-coded personal data.

Recommendation 26

It is recommended that California Penal Code Section 630, et seq. (criminal penalties for unauthorized wiretapping, electronic eavesdropping, intercepting cellular telephone communications, and electronic tracking of individuals) be amended to include all government-issued identification technologies utilizing electronically-coded personal data.

The Radio-Frequency Identification Document Advisory Panel

Senator Simitian asked the California Research Bureau to establish an advisory panel to help it explore issues and recommendations surrounding the use of government issued RFID-enabled identification documents. CRB established an eleven-person Advisory Panel comprised of government officials, industry representatives, and representatives of privacy rights organizations. These groups include organizations focused on

protecting civil liberties, privacy rights, and consumer rights as well as state government, county governments, libraries, and schools. Also included was a representative from the electronics industry, a cryptography security specialist, an electronic security specialist, and an electronic privacy advocate. Table 1 contains the affiliations and names of the members of the panel.

Table 1. Radio Frequency Identification Document Advisory Panel

Civil Liberties	Nicole A. Ozer Technology and Civil Liberties Policy Director American Civil Liberties Union
Privacy Rights	Beth Givens Director Privacy Rights Clearinghouse
Consumers	Leilani Yee Legislative Advocate Consumer Federation of California
Security (cryptography)	Bill Newill Board of Director Security Industry Association
Security (electronic)	Randy Vanderhoof Executive Director Smart Card Alliance
Libraries	Susan Hildreth State Librarian of California
State Government (Information)	J. Clark Kelso California State Chief Information Officer (first meeting) and Federal Receiver in charge of delivering medical care to California Department of Corrections inmates (at the request of Teri Takai, the current State CIO) (second and third meetings)
Electronics Industry	Roxanne Gould Senior Vice President California Government and Public Affairs American Electronics Association
County Government	Steve Keil Director Legislative Services California State Association of Counties (first meeting) and Sacramento County (second and third meetings)
Electronic Privacy Advocate	Jen King Research Specialist Samuelson Law Technology & Public Policy Clinic at U.C. Berkeley School of Law
Schools	Paul Preston Principal Washington Unified School District, West Sacramento

Security and Privacy Recommendations
for Government-Issued
Identity Documents
Using Radio Frequency Identification Tags
or Other Technologies

The Radio-Frequency
Identification Document
Advisory Panel

The panel was established to provide technical advice and best practice approaches to CRB regarding the use of radio-frequency identification (RFID) systems in their many different applications and to outline the strengths and weaknesses of potential approaches to privacy and security using RFID technologies. The Advisory Panel held three meetings: on October 30, 2007, February 6, 2008, and March 10, 2008. The agenda for the first meeting concentrated on identifying issues and solutions regarding RFID technologies

in government-issued identification documents. The panel members were asked to invite speakers to present the issues and recommendations. The general public was also encouraged to speak and to present the panel members with papers. This resulted in the submission of 46 papers, approximately 700 pages in length. Speakers invited by the panel members presented 127 pages of written testimony. A list of the speakers is contained in Table 2.

Table 2. Comments and Testimony Received at First Panel Meeting

Public Comments	
Anne Kelson, Graduate Student, University of California, Davis Valerie Small-Navarro, Senior Advocate, American Civil Liberties Union John Kuester, RFID Global Solution Michelle Tatro, Private Citizen Carol Henton, Vice-President State & Local, Information Technology Association of America Lenny Goldberg, Advocate, Consumer Action & Privacy Rights Clearinghouse Beth McGovern, California Commission on the Status of Women Jeremy Smith, California Labor Federation	
Testimony	
Vulnerabilities of the Technology	<i>Privacy and Security in Radio-Frequency Identification</i> David Molnar, University of California Berkeley, Department of Computer Science <i>RFID Proximity Badge Cloning Demonstration</i> Chris Paget, Independent Security Researcher <i>Soylent Badges: An Attack Surface Analysis of RFID</i> Dan Kaminsky, Independent Security Researcher
Data Security	Joerg Borchert, Vice President Chip Card & Security Integrative Circuits, Infineon Meg Hardon, Senior Policy Director, Infineon <i>Framing the Discussion – Testimony of AeA</i> Ed Howard, Howard Advocacy, Inc.
Impact of Vulnerabilities	<i>RFID and Personal Privacy</i> Lee Tien, Electronic Frontier Foundation <i>Testimony of the National Network to End Domestic Violence</i> Cindy Southworth, Director of Technology, National Network to End Domestic Violence
Comparison to Other ID Options and Technologies Raising Same Concerns	<i>Written Testimony of AIM Global</i> Dan Mullen, AIM Global <i>Different Types of Data Collection/Identification Technologies</i> Kathleen Carroll, Director of Government Affairs, HID Global <i>Privacy Principals for RFID</i> Jim Dempsey, Policy Director, Center for Democracy and Technology

The California Research Bureau highlighted salient points from all testimony received as a result of the first meeting. This information was entered into a database where it was categorized, sorted, and combined. Duplicate issues or recommendations were eliminated.

This process yielded a 22-page document which summarized issues and recommendations that was presented to the panel at its second meeting on February 6, 2008. After discussions received at the meeting, an outline of possible recommendations was prepared and presented at the third and final panel meeting on March 10, 2008. Comments received at that meeting resulted in the development of the 26 recommendations contained in this report.

At the final meeting, a list of goals for the recommendations was presented:

1. Whatever data is stored cannot be read without the knowledge of the user.
2. No more information than necessary should be stored on any machine-readable technology.

3. Users should know what data is contained on the machine readable documents.
4. Document readers should not collect more information than necessary and no more information should be maintained in databases than necessary.
5. The data that is stored on machine readable documents should be difficult or impossible to copy without authorization.
6. Users of identification documents should be given information on how to protect data from being stolen.

Panel members have reviewed a draft of this report, changes were made in response to the comments received, and the panel was provided with a final version of the report. All panel members were given the opportunity to comment in writing on the final draft of the report and their comments are contained in Appendix B.

Justification for Submitted Recommendations

Radio Frequency Identification (RFID) is an electronic system utilized to identify or track items or items. In an RFID identification document, a small memory-storage chip (tag) is embedded. When the document comes within in the range of a receiver/transmitter known as an RFID reader (or emitter), the reader will send out radio waves to detect tags and read the tags data.

This system poses some security/privacy challenges that may be unique to this type of identification document system. According to the Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization, these include:

- **The presence of tags in identification documents may not be apparent.**
- **RFID deployment can lead to the creation of massive databases containing unique tag data.** These records could be linked with personal identifying data, especially as computer memory and processing capacities expand.
- **Hidden readers.** RFID-containing identification documents can be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate.

- **Individual tracking and profiling.** If personal identity were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent.

Even though RFID-containing identification documents may have unique security/privacy issues associated with them, the scope of the recommendations contained in this document were expanded beyond security and privacy recommendations for RFID-enabled government issued identification documents to additional types of identification document systems. The reasons for this are:

1. Most of the concerns or recommendations expressed to the panel did not exclusively apply to RFID technologies.
2. A review of the actions that other governments have taken to address the security and privacy concerns associated with RFID-enabled documents showed that technology-specific approaches to address these concerns are being replaced by processes to address the concerns during system design or before the deployment of a new system.
3. It is difficult to adequately assess the strengths or weaknesses of all current or future machine readable technologies that may be used in an identification document.

Concerns and Recommendations May Not Be Specific to RFID Technologies

Many of the security and privacy concerns expressed testimony received by the Advisory Panel would apply if non-RFID technologies were selected. The initial recommendations received from panel members and the public yielded a total of 140 items. Of these items, 88 (63%) concerned security, privacy, and data management issues that were not specific to government identification systems using RFID technologies. Fifty-two of the 140 items specifically mentioned RFID technologies as either a problem or a specific solution to a government issued identification document or system need. However, many of these 52 items could also apply to a system using other types of machine readable identification document technologies in use today.

What Other Governments Are Doing

The California Research Bureau examined the activities of the European Union and the United States federal governments to determine their most recent activities to address concerns relating to RF-enabled government issued identification documents.

The European Union (EU) is currently engaged in an analysis of the use of RF-technologies that will require specified security and privacy concerns to be addressed when RF technologies are deployed.

All European Union (EU) countries currently issue travel documents, such as passports, containing digital imaging and/or biometrics placed on an RFID chipⁱ. The use of these passports and the belief that the use of RFIDs will increase in the future caused the Commission of the European Communities in 2007 to issue a plan, known as the “Radio Frequency Identification in Europe: Steps Towards a Policy Framework” to adopt a policy framework for the use of RFIDs. The plan states “(t)he specific security and privacy risks largely depend on the nature of the RFID applications: a one-size-fits-all approach would not be able to address the full range of possible applications. Therefore, a close examination of the costs and benefits of specific security and privacy-related risks prior to the selection of RFID systems and the deployment of RFID applications is needed.” The recommendations being prepared pursuant to the directive of the plan are scheduled to be presented to the EU governing bodies at the end of 2008.

On January 29, 2008, the United States Department of Homeland Security issued the final rule for Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes (federal Real ID Act). The final rule states that the security and privacy concerns for the new identification documents (which may not necessarily

ⁱ Specifications for the RFID-enabled passports are contained in: International Civil Aviation Organization (United Nations) “Machine Readable Travel Documents” Part 1, Volume 2 (2006)

**Justification for
Submitted
Recommendations**

contain RF-technologies) needed to be addressed in a comprehensive manner. Under the Real ID Act, States will issue most of the identification documents. The final rule requires that States collect “a minimum of information to be collected by the States to verify identity for issuance of a license or identification card and a minimum of information to be printed on the card and in the machine readable zone.” The final rule goes on to require that the issuing authority submit a security plan explaining how “the personally identifiable information collected, stored, and maintained in DMV records or information systems including a privacy policy is to be accomplished.”

As part of the act, the issuing authority must:

- Issue a clear and understandable privacy policy to each card holder;
- Provide individual access and correction rights for card holders;
- Specify the purpose for collecting personally identifiable information in a privacy policy and limit the use of the data to those purposes;
- Limit the disclosure of the information;
- Require data quality standards and security safeguards to protect against loss or unauthorized access, destruction, misuse, modification, or disclosure;
- Require the performance of a Privacy Impact Assessment, and;
- Require accountability for compliance.

**Assessing the Strengths and Weaknesses of
RFID Technologies**

We attempted to determine if there was a broad consensus on any identified strengths or weaknesses associated with the technology. To accomplish this, we developed a list of topics that were repeatedly identified as strengths or weaknesses associated with the use of RFID technologies in identification systems. Arguments supporting and rebutting each of the reported strengths or weaknesses were either provided by panel members, the public, or are available in reports, journals, and articles.

The validity of the pro or con arguments is not easy to quantify. For example, one of the most widely discussed issues was whether or not it is feasible for an attacker to read an RFID-enabled document without authorization. The panel was presented with evidence that at least some RFID-enabled documents are very difficult, if not impossible, to read without authorization. The panel also watched a demonstration of how easy it was to read at least one kind of RFID, and heard assertions that it may be possible to hack even more sophisticated versions. The outcome of these contests appears to depend on precisely which chip is used, on the environment in which the experiments were conducted, and there was debate about whether the hacking process could be done in a way that would not arouse the suspicion of the user.

The task of evaluating the strengths and weaknesses of RFID-enabled government identification systems is further complicated by the fact that there are so many different varieties of RF-enabled systems and that more are expected to be developed in the future. There are at least three main variants: active, passive, and battery-assisted passive; at least four categories of frequencies with many sub-frequencies exist; there are different standards for the technologies, and RFID

technology standards are developed by more than one widely-recognized standard-setting organization.

With so many variants of what an RFID-enabled identification document can be, it is difficult to assess exactly what the strengths or vulnerabilities of the class of systems that we call “RFID” is or can be. It is further difficult, if not impossible, to predict what types of RFID-enabled systems will be available in the future.

Recommendations

The recommendations were developed for all machine-readable technologies for government-issued identification documents that currently exist or that may be developed in the future and were designed to provide a process to address the security and privacy concerns expressed to the panel. The best practices being studied by the European Union and employed by the federal Real ID Act were used as a basis for some of the recommendations.

The majority of the concerns or recommendations provided to the panel resulted in a broad set of principles that were used to develop specific recommendations. These principles are as follows:

- There should be a demonstrated need for any government agency to change to a new identification system;
- If a new technology is chosen, it should be adequate to meet the need;
- There should be a formal technology assessment that looks at all technologies that can be practically used;
- There should be a feasibility assessment that looks at the costs and benefits of any new technology;
- The effect of a technology choice on a user's data privacy should be considered before a government agency selects a new technology;
- The public should be involved in a selection process;
- The public should be made aware when they are being issued a new technology, they should be provided information on how to use it, how to manage a loss or a theft, and how to dispose of the document when its service life has ended, and;
- The data that is collected, transmitted, or stored should be protected.

Many of the following recommendations contain requirements for local agencies that may trigger the requirement that the State pay the full cost of each mandate, pursuant to Article XIII B, Section 6 of the California State Constitution. This may make the enactment of those recommendations impractical. A legislative option may be to allow the local agencies to opt out via an official action of the legislative body of the local agency.

Several of the recommendations apply to identification documents issued by the University of California (UC). Because of the unique "public trust" status conferred upon UC by Article IX, Section 9 of the California Constitution, it may be necessary for the Regents of the University of California to implement the applicable recommendations.

Recommendation 1

Applicability to K-12 Schools:

It is recommended that the applicability of the state information management principles in this report or contained in Chapter 4800, et seq. (Information Technology) of the State Administrative Manual (SAM) be extended to K-12 public schools as defined in Sections 50-53 of the Education Code. This includes public schools and schools only partly supported by the State, including day and evening elementary and secondary schools.

It is further recommended that the information electronically transmitted from an identification document issued to a California public school K-12 student be limited to the Statewide Student Identifier number issued pursuant to the provisions of Section 49084(e)(3) of the Education Code.

Discussion:

Many of the provisions of the programⁱⁱ that is being recommended by this report are currently required pursuant to Chapter 4800 et. seq. of the State Administrative Manual (SAM), whose statutory authority is derived from Government Code Section 13070. At the current time, the provisions of Chapter 4800 do not explicitly apply to California's K-12 public schools.

It is recommended that Chapter 4800 et. seq. and all new recommendations contained in this report apply to K-12 public schools. Section 4810 of SAM states that the provisions of Chapter 4800 shall apply to State of California departments, offices, boards, commissions, institutions, and special organizational entities. The recommendation is that this applicability definition be expanded to include public schools as defined in Sections 50-53 of the Education Code. This could be accomplished by an amendment to Section 13070 of the Government Code.

ⁱⁱ Some of the recommendations contained in this report (Recommendations 6-9, 11-13, 16-17, and 19-26), if implemented, will require agencies to follow provisions to protect the security and privacy of users of government-issued identification documents that are not currently in Chapters 4800-4900 nor otherwise required.

Recommendations

The Statewide Student Identifier (SSID) is a confidential number assigned to each student pursuant to the provisions of SB 1453 (Alpert, Chapter 1002, Statutes of 2002) that established the California Longitudinal Pupil Achievement Data System to track student achievement. Each K-12 student in a California public school must be assigned an individual, yet non-personally-identifiable SSID. It is recommended that this number may be the most appropriate information to be electronically transmitted from identification documents assigned to K-12 public school students since the use of the number is subject to the privacy protection initiatives of the following:

- Federal Family Educational Rights and Privacy Act (20 U.S.C. Sections 1232g and 1232h and related federal regulations);
- California Education Code related to the maintenance and transfer of student records, particularly Sections 49061 - 49079, inclusive and Sections 49602 and 56347;
- Title 5 of the California Code of Regulations, Sections 430 - 438, inclusive, and;
- The Information Practices Act of 1977 [Chapter 1 (commencing with Section 1978) of Title 1.8 of Part 4 of Division 3 of the Civil Code].

Recommendation 2

Applicability to State Agencies Currently Exempted from State Information Management Principles:

It is recommended that the applicability of the State information management principles in this report or contained in Chapter 4800 et. seq. of the State Administrative Manual be extended to certain State entities currently exempted by Section 4810 of SAM. These

include the University of California, the California State University, community college districts, and the Legislature.

Discussion:

It is recommended that the identity protection provisions in existing State law, and the new provisions in this report, should apply to the University of California, the California State University, the State Compensation Insurance Fund, community college districts, agencies provided by Article VI of the Constitution (judicial entities), and the Legislature.

Recommendation 3

Applicability to Local Agencies:

These recommendations should apply to all “local agencies” when they implement a new government-issued identification system or when they make changes to identification documents or related systems that may create new privacy risks. “Local agencies” are defined in California Government Code Section 6252 and include counties, cities (whether general law or chartered), cities and counties, school districts, and special districts.

Discussion:

The security and privacy risks that can occur with government-issued identification documents can occur whether the document is issued by a State agency or a local government. For this reason, the residents of the State will be better protected if the recommendations in this report also apply to local government entities.

The State of California has established programs for protecting the privacy of its citizens when electronic information technology systems are utilized to collect, transmit, or store confidential information. Many of these programs would apply if a California agency decides to deploy a new or upgraded identification system.

However, no comprehensive program presently exists if the deployment were to be proposed or accomplished by a local agency within the State.

Recommendations

Recommendation 4

Exemption for Agencies:

Agencies should be able to choose to implement new identification systems or modify existing systems without meeting these recommendations where the identification system is only used for internal government operations (when there is no requirement for a member of the general public to obtain or use the identification document) or has been previously assessed under an evaluation similar to that contained in Recommendation 10.

Discussion:

There may be instances when deployment of a new or upgraded government-issued identification document by an agency may not warrant the local agency complying with the stringent provisions proposed by the recommendations contained in this report. For this reason, the exemption contained above was developed.

Recommendation 5

Local government agencies should identify information technology needs during a feasibility study process. As part of the process, the feasibility study should contain the following provisions:

- An analysis of the problem (or opportunity) in terms of its effect on the agency's mission and programs;
- An analysis of the strengths or weaknesses of any existing identification document used by the agency ;
- An identification of the organization's managerial and technical environment within which a response to the problem or opportunity will be implemented;
- Clearly established programmatic and administrative objectives, and;
- Concise functional requirements.

Discussion:

This recommendation would require that local government agencies comply with the requirement for the development of a feasibility study that is required of State Government agencies pursuant to Chapter 4900 of SAM. The specific provisions of

Recommendation 5 are a summary of the requirements contained in Section 4927.

Recommendation 6

All State agencies should consider a range of feasible form factors or features for a new identification document appropriate to the data privacy and security needs of the system in the technology assessment portion of the feasibility study required by Chapter 4900 of SAM. Depending on the functional requirements of the system, the identification document may include, but is not necessarily limited to, the following form factors or features:

- Radio Frequency (RF) Technologies;
- Color Shifting Ink;
- Holograms;
- Microprinting;
- UV Sensitive Printing;
- Magnetic Strips;
- Smart Cards;
- Bar Codes (linear and 2D);
- Watermarks;
- Security Threads;
- Guilloche Printing;
- Color Printing, and/or;
- Serial Numbers.

Discussion:

During the public hearings conducted to obtain information for this report, the recommendation that agencies considering the deployment of a new or upgraded government-issued identification document analyze all types of feasible systems was expressed on several occasions.

Recommendation 7

All State agencies should conduct a privacy impact assessment in the technology assessment portion of the feasibility study required by Chapter 4900 of SAM. In order to assess the impact of the system design upon the data privacy of intended users of the identification document, the privacy impact assessment may include, but not necessarily be limited to:

Recommendations

- What information will be physically or electronically stored or printed on the document;
- What information will be collected and/or stored in the data management system;
- Rationale for the storage and/or printing of the information on the document;
- Why the information is being read, collected, and/or stored by the issuer;
- The intended use of the information;
- With whom the information will be shared (e.g., another agency for a specified purpose);
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information, and how individuals can grant consent, and;
- How the information will be secured (administrative and technological controls) both in the data management system and on the document itself.

Discussion:

The federal E-Government Act of 2002 contains a requirement that a federal agency conduct a “privacy impact assessment” when, among other things, developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form or when initiating a new information technology collection system. Recommendation 7 was based on Section 208, Subsection B. 2. of the E-Government Act of 2002 (Pub. L. No. 107-347, Dec. 17, 2002). Section 208 is contained in its entirety in Appendix D.

Recommendation 8

To assess the impact of the system upon the data privacy of intended users of the identification document, all State agencies should conduct a privacy impact assessment as part of the feasibility study required by Chapter 4900 of SAM. This analysis should include:

- An identification of what choices the agency made regarding the new or modified government-issued identification document system as a result of performing the privacy impact assessment;
- A privacy impact analysis related to systems development, including, as warranted and appropriate, statement of need,

functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, an initial risk assessment;

- An analysis of the impact the system will have on an individual's data privacy, specifically identifying and evaluating potential threats to the extent these elements are known at the initial stages of development, and;
- The privacy impact assessment may need to be updated before deploying the system to consider elements not identified at the concept stage, or to address choices made in designing the system unknown at the time of the initial assessment.

Discussion:

Recommendation 8 was taken from Section II. C. 2. of the Office of Management and Budget's "Guidance for the Implementation of the E-Government Act of 2002", which can be found in its entirety in Appendix E.

Recommendation 9

All State agencies should include an analysis of the following security risks in the feasibility study required by Chapter 4900 of SAM:

- An analysis of the security risks of any known identification document attacks or vulnerabilities and the technologies that counteract those attacks or vulnerabilities. These include, but are not necessarily limited to, the following:
 - Vulnerability of the identification document to cloning;
 - Vulnerability of the identification document to tampering;
 - Vulnerability of the identification document to skimming (using an unauthorized reader to obtain information from the document);
 - Ability to read the data stored on the identification document either legitimately or illegitimately without user knowledge;
 - Vulnerability of the identification document to counterfeiting;
 - Vulnerability of the identification document to spoofing (utilizing a device or devices to transmit electronic data as if it were coming from the actual document);

Recommendations

- Read range (how far away the document can electronically transmit data);
- Vulnerability of the identification document to tracking (the ability to follow a person carrying the document utilizing electronic data being transmitted by the document), and/or;
- Vulnerability of the identification document to replay and relay attacks [In a “replay” attack, an unauthorized person broadcasts an exact re-transmission of a previous legitimate transmission made from a user’s card. In a “relay” attack (otherwise known as a “man in the middle” attack), an unauthorized person receives signals broadcast between a legitimate card and reader and sends those signals to an offsite location to complete an unauthorized transaction].
- An analysis of the necessity of features to ensure adequate defense against security risks not limited to those listed previously, including, but not limited to:
 - Encryption of the data stored on the document;
 - Basic Access Controls, such as the use of a Personal Identification Number (PIN);
 - Authentication between the document and an electronic reader;
 - Radio frequency shielding devices in the event that radio frequency technologies are integrated into the document;
 - On/off switches, and;
 - Opt out/in options.

Discussion:

The lists contained in Recommendation 9 were derived from expressed concerns about RF-enabled documents and recommendations to reduce those concerns that were presented to the Bureau during the advisory panel’s public meetings. While these concerns and recommendations may have the greatest applicability to RFID technologies at the present time, given the rapid advancement of electronic identification technologies, it is probable that the above lists may apply to a higher degree to non-RFID technologies in the future.

Recommendation 10

Local agencies should include the provisions contained in Recommendations 6 through 9 in their feasibility study.

Discussion:

This recommendation is designed to make the feasibility study of local government agencies consistent with those of California State Government agencies.

Recommendation 11

When deploying a new government identification document or system, State and local government agencies should enact rules to ensure that the user's data privacy is protected to the maximum practical extent if the document is reported to be lost or stolen, and should provide the user with information on how to protect security when the document is discarded. The agency should also provide information to holders of new or modified identification documents regarding how the system works and how personal data, if any, will be used or managed:

- The reason that the identification document was issued should be provided;
- The public should be notified which personal information, if any, is stored electronically in the document or is being collected, transmitted, or stored elsewhere;
- The agency should provide a clear description of the privacy or security risks that may be associated with the identification document, and advise on how the user can minimize these risks and an explanation of any rights the user may have to opt out of using the identification document, to restrict the amount of information on the document or to limit its readability, or to otherwise reduce any privacy or security risks associated with its use. Both the risks and the instructions for minimizing risks should be presented in language that a non-technical person can comprehend;
- The agency should maintain a telephone contact number or email address or web site for questions;
- When a document is lost or stolen, the agency should have a process in place to minimize the potential for unauthorized use of

Recommendations

- the document and to limit access to personal information that may be contained within the document, and;
- Agencies should develop procedures for the public to follow to protect the user's privacy and security when disposing of the identification document. These may include, but are not limited to, procedures to deactivate, destroy, or otherwise render the document unreadable or unusable. Members of the public should receive a copy of these procedures when they first get their identification document, and the procedures should be posted on web sites and otherwise accessible later, when they actually need them.

Discussion:

Testimony was received about the importance of ensuring that the public knows how their information is being protected, which information can be potentially compromised, and how to proactively prevent unauthorized use.

As identification documents become more complex and more information than ever can be contained on, or linked to, the document, the potential for identity theft or the unauthorized use of the information increases.

Testimony was also received regarding how difficult it can be to deactivate certain RF and magnetic stripe documents. It is for this reason that we recommend that an issuing agency provide clear instructions to their users regarding how to permanently deactivate an identification document when its service life has ended.

Recommendation 12

State and local government agencies should involve the public in discussions regarding the adequacy of the privacy impact assessment:

- Agencies should publish and distribute a public notice of the proposed privacy impact assessment and a statement of the time, place, and nature of a public hearing. In addition to the general public notice, agencies should attempt to identify and provide notice to groups and individuals with an interest in privacy and technology issues;

Recommendations

- At the public hearing, both oral and written statements should be permitted;
- The agency should consider any comments received and make changes to the privacy impact assessment as warranted;
- The agency should prepare a draft “privacy and security determination statement” summarizing each objection or recommendation regarding the specific amendment proposed together with an explanation of how the final privacy impact assessment has been changed to accommodate each objection or recommendation, or the reasons for making no change. The statement should also contain a written determination that no alternative considered by the agency would be more effective in carrying out the objectives of the new or modified system, and;
- The draft determination statement should be posted and publically noticed by the agency at least 30 days before the agency makes a final determination statement.

Discussion:

Testimony was received regarding the public’s desire to be informed of, and involved in, any decision-making process regarding new or upgraded government-issued identification systems. There is currently no requirement that State or local government agencies have a public hearing, comment period, or substantially involve the public in such a decision making process.

The recommendations above were taken from the public participation component of the Administrative Procedure Act Sections 11346 - 11348, which details a process for involving the public in a decision-making process when amendments or additions to the California Code of Regulations are proposed. The complete text of Sections 11346 – 11348 is contained in Appendix F.

One advisory board member felt that this recommendation is unnecessary and duplicative, since local agencies are already required to participate in local meeting laws that would have a public process that presumably would incorporate most, if not all, of these recommendations.

Recommendations

Recommendation 13

Public notice for the hearing on the proposed privacy impact assessment should be filed with the California Office of Information Security and Privacy Protection, which should distribute the notice to parties it believes to be interested.

Recommendation 14

The draft determination statement shall also be filed with the California Office of Information Security and Privacy Protection.

Discussion for Recommendations 13 and 14:

Testimony was received regarding the difficulty that an agency may have notifying all interested parties when there is an upcoming hearing to discuss the deployment of a new or modified government-issued identification document. The advisory panel also heard about the difficulty that non-profit non-government organizations (NGOs) may have when trying to participate in hearings that may impact their constituents.

It may help increase the visibility of these privacy assessments if notices are sent to, posted, and maintained by a centralized clearinghouse in a manner similar to the environmental documents that are overseen by the Governor's Office of Planning and Research. The mission of the California Office of Information Security and Privacy Protection is aligned with the purpose of the filed documents.

Recommendation 15

It is recommended that Article 8 of the Information Practices Act of 1977 (California Civil Code Sections 1798.30-1798.44) be amended to include local government agencies and the Legislature. The Information Practices Act gives holders of government-issued identification documents the right to inquire as to whether the agency maintains a record about himself or herself and to make those records available. The Act also provides administrative remedies.

Discussion:

This recommendation is being made to make the provisions of this report applicable to all state government agencies as discussed in the rationale for Recommendation 2.

Recommendation 16

It should be the policy of State and local government agencies not to read identification documents without the knowledge of their holders. At locations where a State or local government agency intends to read identification documents that are so sufficiently remote that the identification document holder might be unaware, the agency should alert the user to the location of any devices used by the agency to read the data on the identification document. This recommendation may be satisfied by one or more of the following:

- Posting or displaying a clear and conspicuous sign, placard, poster, or other similar notice at each reader's actual location indicating that the issuing authority has placed an identification document reader at that location, that the reader is being used to read identification documents remotely, and the commonly understood name of each document. The notice might be in the form of a written statement, or it might consist of a widely publicized symbol for an identification document reader;
- Providing each document holder with a list of the location of all readers used or intended to be used by the issuing authority to read the data on the identification document, and/or;
- Providing each document holder with a direct Internet link to a web page that clearly and conspicuously lists the location of all readers used or intended to be used by the issuing authority to read the data on the identification document. This web page shall be kept up to date.

Recommendation 16 will not apply in those instances where the release of a reader's location will pose a security risk to property, if it will increase the likelihood that confidential information will be released, or if the release of the location endangers human life or safety.

Discussion:

Most provisions of this recommendation were taken from Senate Bill 30 (2007-08) which is presented in Appendix A. However, considerable testimony was received stating that it would be unnecessary to post written notices identifying readers that are perfectly obvious to nearly everyone, such as those requiring a close proximity card swipe. Additional signage is needed only

Recommendations

where the reader is sufficiently subtle or novel that a citizen might not know that his or her document was being read. Testimony was also received regarding the possible risk associated with notifying users where a reader is located under certain circumstances, such as in a prison yard. For this reason, we recommend that a requirement to notify users about the location of readers be limited to those circumstances where the reader is not obvious and that there be an exemption if the information may compromise the safety or security of people or property.

Recommendation 17

A state or local government agency should provide the opportunity for the public to offer feedback to the agency about its identification document or system. This should include:

- Providing users a method to comment on the system both prior to and after deployment;
- Providing users a method to report unauthorized use, abuse, or fraud, and;
- The agency should conduct an occasional survey of users after deployment in order to understand any issues or concerns by document users.

Discussion:

Agencies should establish and maintain a feedback mechanism after new identification documents are in use and be prepared to respond to and make changes to the system when required or expedient to do based on user feedback.

Recommendation 18

It is recommended that California Civil Code Section 1798.3(b) (definition of “Agency”) be amended to include local government agencies. This change would make local government agencies subject to California Civil Code Section 1798.29 that requires agencies owning or licensing computerized data containing personal information to disclose any breach of the system’s security to a California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Recommendation 19

A State or local government agency that experiences a breach in its government-issued identification document system should take action to eliminate or substantially reduce the probability of a similar breach occurring within 90 days of the date that the breach occurred.

Discussion for Recommendations 18 and 19:

Testimony was received about the importance of an agency taking quick action to reduce the potentially adverse impacts, such as identity theft, that can occur when a data system containing personal information is breached.

Recommendation 18 will require local government agencies to provide notification of breaches as currently required of State Government agencies.

Recommendation 19 is provided in response to testimony that suggested that a government agency be held accountable for repairing vulnerabilities that were exploited to execute a data breach in their systems and to make necessary modifications in an expeditious manner.

Recommendation 20

For all databases containing information from government-issued identification documents, local government agencies should :

- Identify all automated files and databases for which the agency has ownership responsibility;
- Ensure that responsibility for each automated file or database is defined;
- Enter into agreements with non-State entities that have access to confidential information received from the identification document for security, and;
- Establish appropriate policies and procedures to protect and secure information technology infrastructure

Discussion:

This recommendation would require local government agencies to comply with the information security and integrity provisions that are required of State Government agencies. The requirements for State Government agencies are contained in

Recommendations

Section 4800 of SAM and the provisions of Recommendation 20 were taken from SAM Subsection 4841.2, which is contained in Appendix G.

Recommendation 21

California Penal Code Section 502 is the core definition of “computer crimes” in California law. It is recommended that this section be amended to include government issued identification documents containing electronic data as an input device for “computer systems”.

Recommendation 22

It is recommended that California Penal Code Section 502(c) be amended to include the theft, interference with, or unauthorized access to data from government-issued identification documents containing electronic data as a specific public offense.

Recommendation 23

It is recommended that California Penal Code Section 502(d)(1) be amended to include the public offense noted in Recommendation 22 as a crime punishable by up to 2-3 years of prison and a \$10,000 fine.

Discussion for Recommendations 21-23:

These recommendations are being made in response to testimony suggesting that there be strict penalties for a person obtaining data in an unauthorized manner from government-issued identification cards. The changes proposed in Recommendations 21-23 will make theft, skimming of data, and the unauthorized access of data from a government issued identification document containing electronic data a crime punishable by prison and a fine. These changes will apply to documents that are issued by State and local government agencies.

Recommendation 24

It is recommended that California Penal Code Section 502.6(a) (fraudulent use of information from magnetic stripe credit and debit cards) be amended to include all government-issued identification technologies utilizing electronically-coded personal data.

Recommendation 25

It is recommended that California Civil Code Section 1798.90.1 (drivers license data contained on magnetic stripe) be amended to include all government-issued identification technologies utilizing electronically-coded personal data.

Discussion of Recommendations 24 and 25:

These recommendations are a proposal to update two provisions of existing California law:

1. Include government-issued identification documents containing electronic media in the privacy protection law for credit cards, debit cards, and drivers licenses.
2. Expand the law to include electronic output media other than magnetic stripes.

Recommendation 26

It is recommended that California Penal Code Section 630, et seq. (criminal penalties for unauthorized wiretapping, electronic eavesdropping, intercepting cellular telephone communications, and electronic tracking of individuals) be amended to include all government-issued identification technologies utilizing electronically-coded personal data.

Discussion:

The proposed amendment is designed to deter the skimming of data from the use of government-issued identification documents and the tracking of individuals without their knowledge.

APPENDIX A

TEXT OF SENATE BILL 30 (2007)

BILL NUMBER: SB 30AMENDED
BILL TEXT

AMENDED IN ASSEMBLY AUGUST 31, 2007
AMENDED IN ASSEMBLY JUNE 12, 2007
AMENDED IN SENATE APRIL 19, 2007
AMENDED IN SENATE APRIL 17, 2007

INTRODUCED BY Senator Simitian
(*Coauthor: Assembly Member Leno*)

DECEMBER 4, 2006

An act to add Article 4 (commencing with Section 1798.10) to Chapter 1 ~~to~~ of Title 1.8 of Part 4 of Division 3 of the Civil Code, and to add Article 13 (commencing with Section 11147) ~~of~~ to Chapter 1 of Part 1 of Division 3 of Title 2 of the Government Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 30, as amended, Simitian.

Identity Information Protection Act of 2007.

(1) Existing law, the Information Practices Act of 1977, regulates the collection and disclosure of personal information regarding individuals by State agencies, except as specified. The intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the act is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains. This bill would enact the Identity Information Protection Act of 2007. Until December 31, 2012, or as otherwise specified, the act would require identification documents, as defined and with specified exceptions, that are created, mandated, purchased, or issued by various public entities that use radio waves to transmit data, or to enable data to be read remotely, to meet specified requirements. The bill would require those public entities and authorized 3rd parties to protect operational system keys and data transmitted remotely by those identification documents from unauthorized access, and would restrict the disclosure thereof. The bill would authorize declaratory or injunctive relief or a writ of mandate and attorney's fees and costs under specified circumstances. Because the intentional disclosure of medical, psychiatric, or psychological

information in violation of the disclosure provisions of the Information Practices Act of 1977, which would include this act, is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains, this bill would expand the scope of an existing crime, thereby imposing a State-mandated local program.

(2) Existing law establishes in the Department of Consumer Affairs, the Office of Privacy Protection for the purpose of protecting the privacy of individuals' personal information and developing fair information practices for State agencies. Existing law establishes in the California State Library, the California Research Bureau with responsibilities to conduct research on various policy issues. This bill would require the California Research Bureau to submit a report to the Legislature on security and privacy for government-issued, remotely readable identification documents. The bill would require the bureau to submit the report within 270 days of receiving a request from the Office of the President pro Tempore of the Senate or the Office of the Speaker of the Assembly, or before June 30, 2008, whichever is earlier. The bill would require the bureau to establish an advisory board, to be comprised of specified government officials and representatives from industry and privacy rights organizations, to make recommendations and provide technical advice to the bureau in preparing the report.

(3) The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement. This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. This act shall be known and may be cited as the Identity Information Protection Act of 2007. SEC. 2. The Legislature hereby finds and declares all of the following:

(a) The right to privacy is a personal and fundamental right protected by Section 1 of Article I of the California Constitution and by the United States Constitution. All individuals have a right of privacy in information pertaining to them.

(b) This state has previously recognized the importance of protecting the confidentiality and privacy of an individual's personal information contained in identification documents such as driver's licenses.

(c) It is the intent of the Legislature that the privacy and security protections in this article that apply to remotely readable identification documents created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof, are interim measures until subsequent legislation or regulations are enacted based on new information, including, but not limited to, information provided by the California Research Bureau.

(d) Notwithstanding any other provision of this act, it is the intent of the Legislature that the interim measures contained herein be replaced by a statewide legislative or regulatory framework in the most timely and expeditious fashion possible following the issuance of

Appendices

recommendations by the California Research Bureau. SEC. 3. Article 4 (commencing with Section 1798.10) is added to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, to read:

Article 4. Identity Documents

1798.10. (a) Except as provided in subdivision (b), all identification documents created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof, that use radio waves to transmit data or to enable data to be read remotely shall meet these requirements:

- (1) In order to prevent duplication, forgery, or cloning of the identification document, the identification document shall incorporate tamper-resistant features.
- (2) In order to determine to a reasonable certainty that the identification document was legitimately issued by the issuing entity, is not cloned, and is authorized to be read, the identification document and authorized reader, in conjunction with related, functionally integrated software, shall implement an authentication process.
- (3) If personal information is transmitted remotely from the identification document, the identification document and authorized reader, in conjunction with related, functionally integrated software, shall not only meet the requirements of paragraph (2) but also shall implement mutual authentication in order to prevent the transmission of personal information between identification documents and unauthorized readers.
- (4) If personal information is transmitted remotely from the identification document, the identification document shall make the data unreadable and unusable by an unauthorized person through means such as encryption of the data during transmission, access controls, data association, encoding, obfuscation, or any other measures, or combination of measures, that are effective to ensure the confidentiality of the data transmitted between the identification document and authorized reader.
- (5) If personal information is transmitted remotely from the identification document, the identification document shall implement an access control protocol that enables the holder to exercise direct control over any transmission of the data using radio waves. This requirement may be satisfied by the implementation of one or more means including, but not limited to, the following:
 - (A) An access control protocol requiring the machine-readable or other nonradio frequency reading of information from the identification document prior to each transmission of data using radio waves, without which the identification document will not transmit data using radio waves.
 - (B) A data carrying device, such as an integrated circuit or computer chip, that is normally not remotely readable, accessible, or otherwise operational under any circumstances, and only remotely readable, accessible, or operational while being temporarily switched on or otherwise intentionally activated by a person in physical possession of the identification document. The device shall only be remotely readable while the person intentionally enables the identification document to be read.

- (C) Another access control protocol that enables the holder to exercise direct control over any transmission of the data using radio waves, not including a detachable shield device or bag.
- (6) If a unique personal identifier number that is used to provide an individual with access to more than one type of application or service is transmitted remotely from the identification document, the issuing entity of the identification document shall do one or more of the following, commensurate with the sensitivity of the applications:
- (A) Implement a secondary verification and identification procedure that does not use radio waves, including, but not limited to, the manual entry of a personal identification number on a keypad or the placement of an authorized individual at locations at which the identification document is to be read for a purpose other than facilitating secured access to a secured public building or parking area, in order to determine the authenticity of the document or the identity of the person.
- (B) Implement the security protections described in paragraph (3).
- (C) Implement the security protections described in paragraph (4).
- (D) Implement the security protections described in paragraph (5).
- (7) If the identification document remotely transmits a unique personal identifier number for the purposes of recording the attendance of a pupil at a public school, the issuing entity of the identification document shall meet the requirements of paragraph (6).
- (8) If the identification document remotely transmits a unique personal identifier number for the purposes of accessing public transit services, is issued to a member of the public, as defined in Section 6252 of the Government Code, and is either required by the issuing public entity or confers a benefit that is unique to that class of remotely readable identification document, the issuing entity of the identification document shall meet the requirements of paragraph (6).
- (9) The issuing entity of the identification document shall communicate in writing to the person to whom the document is issued at or before the time the document is issued, all of the following:
- (A) That the identification document can transmit data or enable data to be read remotely without his or her knowledge.
- (B) That countermeasures, such as shield devices or switches, may be used to help the person control the risk that his or her data will be read remotely without his or her knowledge.
- (C) The location of readers used or intended to be used by the issuing authority to read the data on the identification document. This requirement shall be satisfied by doing one or more of the following:
- (i) Posting or displaying a clear and conspicuous sign, placard, poster, or other similar written notice at each reader's actual location indicating that the issuing authority has placed an identification document reader at that location, that the reader is being used to read identification documents remotely using radio waves, and the commonly understood name of each document.
- (ii) Providing each document holder with a list of the location of all readers used or intended to be used by the issuing authority to read the data on the identification document.

Appendices

(iii) Providing each document holder with a direct Internet link to a web page that clearly and conspicuously lists the location of all readers used or intended to be used by the issuing authority to read the data on the identification document. This web page shall be updated regularly.

(D) All circumstances under which the issuing authority plans or intends to read the identification document and the reasons behind those circumstances.

(E) Any information, such as time and location that is being collected or stored regarding the individual in a database at the time the identification document is being read.

(b) Subdivision (a) shall not apply to:

(1) Any contactless identification document system that began implementation prior to January 1, 2008, or for which a state, county, or municipal government request for proposal has been publicly issued prior to September 30, 2007, or for which a contract has been executed prior to September 30, 2007.

(2) An identification document issued to a person who is incarcerated in the state prison or a county jail, detained in a juvenile facility operated by the Division of Juvenile Facilities in the Department of Corrections and Rehabilitation *or a county probation department*, or housed in a mental health facility, pursuant to a court order after having been charged with a crime, or to a person pursuant to court-ordered electronic monitoring.

(3) An identification document issued to a person employed by a state prison, county jail, or juvenile facility operated by the Division of Juvenile Facilities in the Department of Corrections and Rehabilitation if the document is not removed from the facility and the requirements of paragraph (9) of subdivision (a) apply.

(4) An identification document issued to a law enforcement officer or emergency response personnel if the document is used only while the law enforcement officer or emergency response personnel is on active duty and the requirements of paragraph (9) of subdivision (a) apply.

(5) An identification document issued to a patient who is in the care of a government-operated or government-owned hospital, ambulatory surgery center, or oncology or dialysis clinic if all of the following requirements are met:

(A) The identification document is valid for only a single episode of care.

(B) The identification document may be removed and reattached when used on a nonemergency outpatient.

(C) The identification document does not transmit or enable the remote reading using radio waves of personal information.

(D) The patient returning for a new episode of care is assigned a new unique personal identifier number.

(E) The patient or the person who has been legally entrusted to make medical decisions on behalf of the patient is notified, in writing, that the identification document transmits data using radio waves.

- (F) The patient is not compelled or encouraged to wear, or keep on his or her person, the identification document beyond the facility property.
- (6) An identification document issued to a person who is in the care of a skilled nursing facility operated or owned by the government, if all of the following requirements are met:
- (A) The patient has been diagnosed by a doctor with dementia or other cognitive impairment that involves substantial limitation in function.
- (B) The identification document does not transmit or enable the remote reading using radio waves of personal information.
- (C) The patient or the person who has been legally entrusted to make medical decisions on behalf of the patient is notified, in writing, that the identification document transmits data using radio waves.
- (D) The patient is not compelled or encouraged to wear or keep on his or her person the identification document beyond the facility property.
- (E) The patient or the person who has been legally entrusted to make medical decisions on behalf of the patient has consented to the issuance of the identification document.
- (7) An identification document issued to a patient by emergency medical services for triage or medical care during a disaster and immediate hospitalization or immediate outpatient care directly related to a disaster, as defined by the local emergency medical services agency organized under Section 1797.200 of the Health and Safety Code.
- (8) An identification document that is issued to a person for the limited purpose of facilitating secured access by the identification document holder to a secured public building or parking area, if the requirements of paragraph (9) of subdivision (a) are met and the identification document does not transmit or enable the remote reading using radio waves of personal information.
- (9) A license, certificate, registration, or other authority for engaging in a business or profession regulated under the Business and Professions Code, if the requirements of paragraph (9) of subdivision (a) are met and the identification document does not transmit or enable the remote reading using radio waves of personal information.
- 1798.11. Except as provided in subdivision (d), a state, county, or municipal government, or subdivision or agency thereof, that creates, mandates, purchases, or issues an identification document in compliance with subdivision (a) of Section 1798.10:
- (a) Shall not, under any circumstances, disclose any operational system keys used pursuant to paragraphs (3) and (4) of subdivision (a) of Section 1798.10, either publicly or to any nongovernmental entity or other third party, including, but not limited to, contractors, officers, and employees of other government agencies, that is not authorized under subdivision (d).
- (b) Shall take all reasonable measures to keep any operational system keys used pursuant to paragraphs (3) and (4) of subdivision (a) of Section 1798.10 secure and unavailable to any third party that is not authorized under subdivision (d).
- (c) Shall not, under any circumstances, act in any way to allow a third party that is not authorized under subdivision (d) to read the data transmitted remotely by the identification document using radio waves.

Appendices

(d) A state, county, or municipal government, or subdivision or agency thereof, that creates, mandates, purchases, or issues an identification document in compliance with subdivision (a) of Section 1798.10 may disclose any operational system keys used pursuant to paragraphs (3) and (4) of subdivision (a) of Section 1798.10 to authorized third parties that in the stream of commerce have a bona fide business relationship with the agency, or its contractors or subcontractors, and that are necessary to the operation, testing, or installation of the identification system, and to emergency response personnel for the sole purposes of locating and identifying a person or persons in the case of a disaster, as defined by the local Emergency Medical Services agency organized under Section 1797.200 of the Health and Safety Code.

(1) Any authorized third party that receives a disclosure pursuant to this exception is subject to the prohibitions of subdivisions (a) to (c), inclusive.

(2) Any authorized third party that receives a disclosure pursuant to this exception shall adopt procedures restricting access to the operational system keys and securing the keys from tampering and unauthorized access. These procedures shall include administrative, technical, and physical safeguards to protect against any reasonably anticipated threats or hazards to the privacy of the information, and unauthorized uses or disclosures of the information.

(3) All information received pursuant to this exception shall be destroyed when the purpose of the disclosure is completed.

1798.12. A state, county, or municipal government, or a political subdivision or agency thereof, that uses radio waves to transmit data or to enable data to be read remotely pursuant to subdivision (a) of Section 1798.10 or the authorized third parties with whom the governmental entity has a bona fide business relationship shall not disclose any data or information regarding the location of a person derived from the use of the radio waves, unless the disclosure comports with any of the following:

(a) The disclosure is made pursuant to an exigent circumstance and all of the following occur:

(1) The information that is requested is necessary to locate and respond to a person who is in immediate danger of death or serious bodily injury or a minor who is in immediate danger.

(2) The information that is disclosed solely regards the location of a person or an identification document and the time at which that person was or is at that location.

(3) The request by emergency response personnel to a governmental entity to which this section applies includes, at a minimum, all of the following information:

(A) The name and title of the emergency response personnel.

(B) The office location and telephone number for the emergency response personnel.

(C) The name and telephone number of the emergency response personnel's supervisor or the person who has the ultimate operational responsibility at the time.

(D) The assertion by the emergency response personnel that an exigent circumstance exists.

(4) The governmental entity provides the emergency response personnel with the requested location information upon verification of the information required by paragraph (3) with the emergency response personnel's supervisor or the person who has ultimate operational responsibility at the time. No governmental entity, or official or employee thereof, shall be

subject to liability when it acts in a reasonable manner upon receiving the information required by paragraph (3).

(5) The governmental entity maintains for a period of not less than one year all requests from public safety or emergency response agencies for location information that are made under exigent circumstances.

(6) Individuals whose location information has been released pursuant to this subdivision are notified in writing by the governmental entity within a reasonable period of time that their information has been released and the notice shall include the information required in paragraph (3). The notification required by this paragraph may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this paragraph shall be made after the law enforcement agency determines that it will not compromise the investigation.

(7) The location information obtained as the result of a request pursuant to this section is used solely for the purpose of rendering emergency aid by emergency response personnel to the person during the exigent circumstances forming the basis of the request.

(b) The disclosure is required pursuant to a search warrant.

1798.125. Any interested person may institute proceedings against a governmental entity for injunctive or declaratory relief or a writ of mandate in any court of competent jurisdiction for the purpose of preventing or stopping any violation of this article, if all of the following occur:

(a) The person provides to the governmental entity, written notice of the alleged violation by certified mail.

(b) The governmental entity fails, for at least 30 days after receipt of that written notice, to fix the alleged violation, to comply with the provisions of the article, and to inform the demanding party in writing of its actions to fix the alleged violation or its decision not to correct the alleged violation.

1798.126. (a) In any proceedings brought pursuant to Section 1798.125, the court may assess against the governmental entity reasonable attorney's fees and other litigation costs reasonably incurred in any proceedings under this article in which the complainant has prevailed.

(b) Nothing in this section affects or is intended to limit or supplant any other remedies that may be available in law or equity.

1798.135. For purposes of this article, the following definitions shall apply:

(a) "Access controls" means granting or denying permission to access information.

(b) "Authentication" means the process of applying a machine-readable process to data or identification documents, or both, so as to accomplish either of the following:

(1) Establish that the data and the identification document containing the data were issued by the responsible issuing state or local governmental body.

(2) Ensure that a reader, as defined in subdivision (p), is permitted under California law to access that data or identification document.

(c) "Authorized reader" means a reader, as defined in subdivision (p), that, with respect to a particular identification document, (1) is permitted under California law to remotely read the

Appendices

data transmitted by that identification document, (2) is being used for a lawful purpose, and (3) is fully in accord with the requirements of subdivision (a) of Section 1798.10.

(d) "Contactless identification document system" means a group of identification documents issued and operated under a single authority that use radio waves to transmit data remotely to readers intended to read that data. In a contactless identification document system, every reader must be able to read every identification document in the system.

(e) "Data" means information stored on an identification document in machine-readable form including, but not limited to, personal information and other unique personal identifier numbers.

(f) "Data association" means storing information in separate locations so that the information is not resident in a single location and is not usable if only one of such locations is accessed.

(g) "Emergency response personnel" means any of the following:

(1) "Emergency medical technician," as defined in Sections 1797.80 and 1797.82 of the Health and Safety Code.

(2) "Firefighter," as defined in Section 1797.182 of the Health and Safety Code.

(3) "Mobile intensive care nurse," as defined in Section 1797.56 of the Health and Safety Code.

(4) "Paramedic," as defined in Section 1797.84 of the Health and Safety Code.

(5) "Peace officer," as defined in Sections 830.1 and 830.2 of the Penal Code.

(h) "Encoding" means use of a mechanism that allows the message elements to be substituted for other elements.

(i) "Encryption" means the protection of data in electronic form in storage or while being transmitted using an encryption algorithm implemented within a cryptographic module that has been adopted or approved by the National Institute of Standards and Technology, the Institute of Electrical and Electronics Engineers, Inc., the Internet Engineering Task Force, the International Organization for Standardization, the Organization for the Advancement of Structured Information Standards, or any other similar standards setting body, rendering that data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of that data. That encryption shall include appropriate management and safeguards of those keys to protect the integrity of the encryption.

(j) "Exigent circumstance" means a reasonable belief by emergency response personnel that either of the following situations exists:

(1) There is immediate danger of death or serious bodily injury to the person whose location information is being sought or to another individual who could be located through the reading of that identification document.

(2) There is immediate danger to a minor whose location information is being sought or to another minor who could be located through the reading of that identification document.

(k) (1) "Identification document" means any document containing data that is issued to an individual and which that individual, and only that individual, uses alone or in conjunction with any other information for the primary purpose of establishing his or her identity.

Identification documents specifically include, but are not limited to, the following:

- (A) Driver's licenses or identification cards issued pursuant to Section 13000 of the Vehicle Code.
- (B) Identification cards for employees or contractors.
- (C) Identification cards issued by educational institutions.
- (D) Health insurance or benefit cards.
- (E) Benefit cards issued in conjunction with any government-supported aid program.
- (F) Licenses, certificates, registration, or other means to engage in a business or profession regulated by the Business and Professions Code.
- (G) Library cards issued by any public library.
- (2) Identification documents do not include devices issued to persons for the limited purpose of collecting funds for the use of a toll bridge or toll road, such as devices used by the FasTrak system, if the device is not issued for the exclusive use of an individual and does not transmit or enable the remote reading using radio waves of personal information.
- (l) "Key" means a string of bits of information used as part of a cryptographic algorithm used in encryption.
- (m) "Mutual authentication" means a process by which identification documents and authorized readers securely challenge each other to verify authenticity and authorization of both readers and documents before any data is exchanged, except such data as is necessary to carry out mutual authentication. Mutual authentication accomplishes both of the following:
 - (1) Authorized readers, as defined in subdivision (c), can accurately assess whether the identification document and data stored are issued by the responsible issuing state or local governmental body to an authorized holder.
 - (2) Authorized identification documents can accurately assess whether a reader accessing them is authorized to read the documents, and authorized to then access data stored on the documents.
- (n) "Obfuscation of information" means the transformation of information without the use of an encryption algorithm or key into a form in which the information is rendered unusable or unreadable.
- (o) "Personal information" includes any of the following data elements to the extent that they are used alone or in conjunction with any other information to identify an individual:
 - (1) First or last name.
 - (2) Address.
 - (3) Telephone number.
 - (4) E-mail address.
 - (5) Date of birth.
 - (6) Driver's license number or California identification card number.
 - (7) Any unique personal identifier number contained or encoded on a driver's license or identification card issued pursuant to Section 13000 of the Vehicle Code.
 - (8) Bank, credit card, or other financial institution account number.
 - (9) Credit or debit card number.

Appendices

(10) Any unique personal identifier number contained or encoded on a health insurance, health benefit, or benefit card issued in conjunction with any government-supported aid program.

(11) Religion.

(12) Ethnicity or nationality.

(13) Photograph.

(14) Fingerprint or other biometric identification.

(15) Social security number.

(p) "Reader" means a scanning device that is capable of using radio waves to communicate with an identification document and read the data transmitted by that identification document.

(q) "Remotely" means that no physical contact between the identification document and a reader is necessary in order to transmit data using radio waves.

(r) "Shield devices" mean physical or technological protections available to stop the transmission of data programmed on or into an identification document using radio waves.

(s) "Single episode of care" means an inpatient hospital stay through discharge or specific course of therapy or treatment for outpatient care.

(t) "Unique personal identifier number" means a randomly assigned string of numbers or symbols that is encoded onto the identification document and is intended to identify the identification document that has been issued to a particular individual.

1798.136. The provisions of this article shall become inoperative on December 31, 2012, or when alternative statewide regulations pertaining to the privacy and security of remotely readable identification documents are enacted or promulgated pursuant to later legislation, whichever is earlier.

SEC. 4. Article 13 (commencing with Section 11147) is added to Chapter 1 of Part 1 of Division 3 of Title 2 of the Government Code, to read:

Article 13. Report on Security and Privacy for Government-Issued Identification Documents 11147. The California Research Bureau in the California State Library, within 270 days of receiving a request from the Office of the President pro Tempore of the Senate or the Office of the Speaker of the Assembly, or before June 30, 2008, whichever is earlier, shall submit to the Legislature a report on security and privacy for government-issued, remotely readable identification documents.

11147.1. In preparing the report required by Section 11147, the bureau shall, at a minimum, do all of the following:

(a) Establish an advisory board that makes recommendations, provides technical advice, answers bureau questions, and outlines the strengths and weaknesses of potential approaches to privacy and security proposals for government-issued, remotely readable identification documents. The advisory board shall be composed of all of the following members:

(1) The State Chief Information Officer or his or her designee.

(2) The Chief of the Office of Privacy Protection or his or her designee.

(3) The Attorney General or his or her designee.

- (4) A representative from the Office of Emergency Services.
- (5) A representative from either the University of California or the California State University system.
- (6) A representative from the Department of Motor Vehicles.
- (7) A representative from the California State Information Security Office.
- (8) A representative selected by the bureau from the California School Boards Association.
- (9) A representative selected by the bureau from city or county government.
- (10) One representative selected by the bureau, from each of the following industries:
 - (A) Remotely readable identification card manufacturers.
 - (B) Remotely readable identification chip manufacturers.
 - (C) Remotely readable identification reader manufacturers.
 - (D) Remotely readable component manufacturers.
 - (E) Enterprise or network information technology companies.
- (11) Five representatives selected by the bureau from among privacy rights groups, including, but not limited to, the American Civil Liberties Union, the Electronic Frontier Foundation, and the Privacy Rights Clearinghouse.
- (12) Other representatives selected by the bureau that would be necessary for the bureau to complete the report required by Section 11147.
 - (b) Review and document existing state and federal laws relating to privacy, security, and safeguards for remotely readable identification documents.
 - (c) Review privacy and security safeguards and technologies that are currently available or in development for remotely readable identification documents.
 - (d) Review best practices that have been established or that are under consideration to prevent identity theft, privacy invasion, and criminal use of personal and other data to determine their applicability to government-issued identification documents.
 - (e) Consider requirements for a privacy impact assessment and a security risk assessment conducted by issuing entities that would clearly define what personal information is to be collected, how the information will and could be used, who may and who could access the information, how the information will be protected from unauthorized access, and how an individual may control use of and update his or her information.
 - (f) Identify, develop, and evaluate options for the Legislature to review and consider for action for a legislative and regulatory framework that would ensure the safety and security of information contained on remotely readable identification documents and the privacy of the individuals to whom the documents are issued.

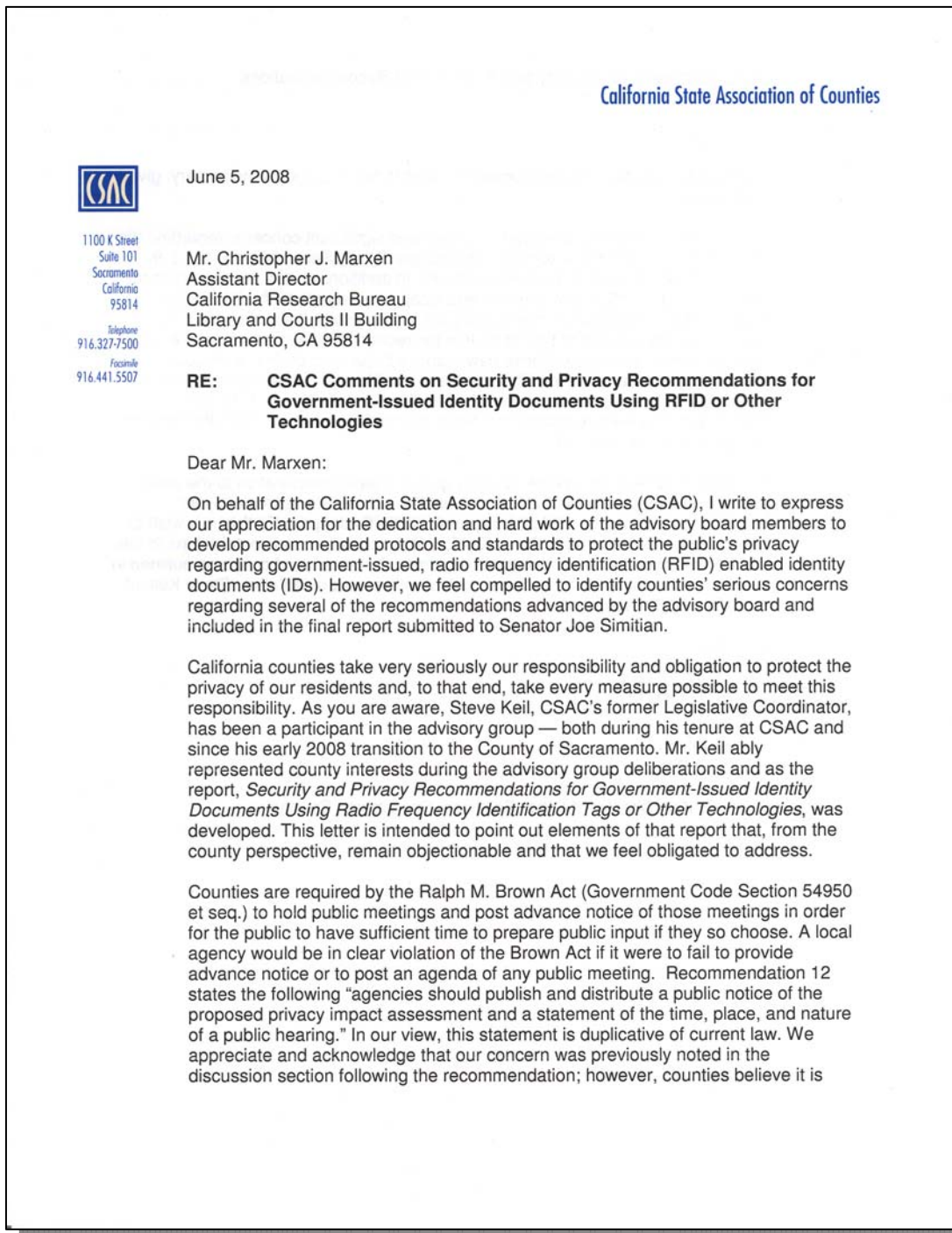
11147.2. The bureau shall be solely responsible for preparing the report required by this article. The report shall include information, suggestions, and comments from the advisory board. In making recommendations, the bureau shall maintain an approach that, when appropriate, is neutral with respect to specific technologies and methods, shall consider the multitude of ways of ensuring privacy and security, and shall consider the impact of any recommendations on innovation. The report may include additional research and commentary that the bureau believes is necessary to prepare a complete and thorough report.

Appendices

SEC. 5. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

APPENDIX B

RADIO-FREQUENCY IDENTIFICATION DOCUMENT ADVISORY PANEL COMMENT



Security and Privacy Recommendations
for Government-Issued
Identity Documents

Appendices

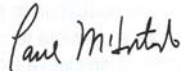
CSAC Comments on Security and Privacy RFID Recommendations
Page 2 of 2

important to reiterate that this recommendation is not, in our view, necessary, given existing law.

Furthermore, it must be noted that counties have significant concerns regarding the cost of implementing the recommendations, specifically Recommendations 5-9, 12, 16, and 19-20, directed at local governments. In addition, we are concerned about Recommendation 15, which seeks to add local governments to the Information Practices Act. If these recommendations are implemented, it should have been made clear at the outset of the report that the recommendations contain new and significant mandated costs. These new responsibilities and duties need to be identified as reimbursable mandates or there must be opt-out provision offered. We would note that public agencies would, in all likelihood, lobby against those provisions if they were to appear in a future piece of legislation, unless the issue of mandated costs is resolved.

On behalf of CSAC, we ask the advisory group to give consideration to the local government perspective on the issues identified above. We appreciate your including our comments within the appendix of the final report. Further, we wish to take the opportunity to thank Steve Keil for his participation and contributions to this effort. Should you have any questions regarding the issues and concerns outlined in this letter, I ask that you make direct contact with our representative, Steve Keil, at (916) 874-6887. Thank you.

Sincerely,



Paul McIntosh
Executive Director

cc: Steve Keil, Director of Labor Relations, Sacramento County

California State Public Policy



June 6, 2008

Chris Marxen
Assistant Director
California Research Bureau
900 N Street, Suite 300
Sacramento, CA 95814

Re: Comments of the American Electronics Association

Dear Chris Marxen:

On behalf of the AeA (American Electronics Association, please find the following recommendations regarding the final draft of the California Research Bureau RFID Document:

**Security and Privacy Recommendations for
Government-Issued Identity Documents
Using Radio Frequency Identification Tags
or Other Technologies**

COMMENTS OF THE AMERICAN ELECTRONICS ASSOCIATION¹

AeA's October testimony to the Bureau made four main points:

1. AeA argued that, in the practical, real world, radio frequency identification (RFID) technologies exist side-by-side with other, competing options available to procurement officials. These other options, in turn, have their own vulnerabilities and cost. Hence:

"It is in our opinion disingenuous to discuss the privacy challenges of any particular technology without an accompanying and honest assessment of the vulnerabilities of the existing alternatives. Thus, to discuss the vulnerabilities of RFID without also weighing the vulnerabilities of bar codes, magnetic strips, biometrics, passwords, and guards looking at a photo ID is to erect a massive straw man where, because RFID is legislatively approached in isolation, the misimpression is created that it is riskier than those technologies not discussed."

2. AeA also argued that micro-managing, highly prescriptive legislatively-mandated solutions (e.g., mandating a level of encryption or Faraday cages in code) were misguided. As we stated in our testimony:

"what separates the parties in the RFID debate is not whether there are privacy challenges posed by RFID. Every form of communication carries with it the risk that private information can be communicated...Rather, what separates the parties is whether those challenges are unprecedented warranting unprecedented legislative micro-management dictating to government agencies how they must procure an evolving, potentially beneficial technology that can be used in a variety of ways in a variety of settings."

3. Reinforcing the need to avoid one-size-fits-all micro-managing legislative prescriptions was our point that RFID itself is so varied and flexible that such prescriptions cannot credibly be written for RFID even if it was wrongly considered in isolation:

¹ At the outset, AeA would like to thank Mr. Chris Marxen of the California Research Bureau for all of his hard work; the other members of the Radio-Frequency Identification Document Advisory Panel for their collegiality, perspectives, and willingness to serve; and Senator Similtan for his receptivity to a process that permitted a more detailed and substantive discussion than is often found in legislative hearings and debates.

1415 L Street, Suite 1260 / Sacramento, CA 95814 / P 916.443.9059 / F 916.443.6734

www.aeonet.org

Security and Privacy Recommendations for Government-Issued Identity Documents

Appendices

"[RFID] technology itself can and should be proportionally scaled to safeguard data stored on the chip, based on the level of risk that personal information could be compromised and the cost of protecting against that risk."

4. Finally, AeA set forth its list of "Best Practices," then observed:

All of these policies together represent a sliding scale of privacy protection. The more personal the information – the more it inherently can be used to identify a particular individual – the greater the protection that should be considered. But, to observe that the neighborhood bank has fewer protections than Fort Knox is not to indict the neighborhood bank as insecure requiring legislative micro-management of bank architecture. Each must be assessed and judged situationally, based on an assessment of use and hence risk.

Crucially, and laudably, the Recommendations do *not* single out RFID; do *not* propose legislation seeking to mandate enumerated kinds of privacy-protection strategies; and *they do* propose a means for making situational assessments grounded in the same principles AeA identified in its "Best Practices." On these grounds, we applaud the Recommendations, especially its key conclusion that:

"Even though RFID-containing identification documents may have unique security/privacy issues associated with them, the scope of the recommendations contained in this document were expanded beyond security and privacy recommendations for RFID-enabled government issued identification documents to additional types of identification document systems. The reasons for this are:

1. Most of the concerns or recommendations expressed to the panel did not exclusively apply to the use of RFID technologies
2. A review of the actions that other governments have taken to address the security and privacy concerns associated with RFID-enabled documents shows that technology-specific approaches to address these concerns are being replaced by processes to address the concerns during system design or before the deployment of a new system
3. It is difficult to adequately assess the strengths or weaknesses of all current or future machine readable technologies that may be used in an identification document."

Yet, while the Recommendations in the main adopt AeA's four main points, in our view responsible decision-makers must still oppose them. Here is why: the Recommendations suggest a highly detailed, time-intensive, and thus extremely costly plan for evaluating and obtaining public input where the procurement of *new* identification credentials is concerned. But, the Recommendations do not clearly require state or local agencies to perform a similar evaluation of current, potentially obsolete, *incumbent* technologies. (See, e.g., Recommendation # 11's reference to "new.")

Because the Bureau's proposals appear to apply only to new procurements, it is self-evident that agencies will have an overwhelming incentive to do nothing new at all, even if the incumbent technology is perilously obsolete; even if new technology could be far more protective of privacy; even if new technology will save the agency money by reducing fraud and increasing efficiency in the mid-to-long term. For anyone familiar with California's already labored technology procurement process, this fear is not conjecture but hardened fact.²

For this reason the regrettable but wholly inevitable practical impact of the Recommendations will be to *frustrate and undermine the very values the Recommendations strive to advance*. Enhanced privacy, thoughtful consideration of ID procurement implications, and better security – each will be thwarted as the Recommendations unwittingly freeze cash-strapped agencies in time while those who scheme to invade privacy and break security are not so constrained, constantly updating their tactics and strategies with the benefit of the latest advances.³

² One example cited at a recent Senate Budget hearing was that 9 of the last 10 major IT procurements had one bidder. This is because of the hugely expensive, cumbersome and uncertain nature of procurements now without those additional steps proposed by the Bureau. We don't force companies to bid. The procurement system must make it literally and predictably worth their while which means, at minimum, to entice bidders, it can't be too long or too costly.

³ We understand that the Bureau believes incumbent systems would in fact have to go through the privacy assessments suggested by the report. For the reasons just articulated, we hope that is the case. Yet, none of our members who reviewed this draft came to that conclusion and we believe that is a fair forecast of how future readers will interpret the scope of the report. If the intent is to require incumbent technologies to be included, then an explicit statement would be welcome.

Our other more specific suggestions are as follows:

Recommendation #4: This Recommendation appears to be consistent with the explanation Bureau staff provided during the panel discussions, but would be much clearer if the heading read "Exemption for State and Local Agencies." Doing so will provide consistency and clarity to the document.

Recommendation #6: Imagine a list of recording equipment twenty years ago: reel-to-reel, eight-track, laserdisc, cassette. Requiring state agencies consider a range of design features to consider when procuring ID credentials is valid but listing a random group of technologies that might be reviewed in a study is prejudicial and will quickly be out-of-date. Those with experience in procurements know that literal-minded procurement officials will waste time considering each listed technology even if obviously dated or inapplicable. A principled document like that offered by the CRB should not be, even indirectly, endorsing one technology or concept or design over another by its inclusion in this list. The list is inevitably obsolete almost immediately as evidenced by the fact that the list described in the CRB paper does not reflect technologies that have been developed and perfected in the short few weeks since it was drafted.

Recommendation #7: A privacy impact assessment should be conducted as part of the feasibility study (Recommendation #5), and should not duplicatively and sequentially follow the evaluation of system design. The Recommendations here in #7 are purportedly directed at system design, but that could include what information is on the credential. A secure and privacy-protecting ID system will include a privacy impact assessment on the entire ID management process, including the credential as an extension of the system.

Recommendation #8: It is very difficult to distinguish the recommendations in 8 from 7 and from the overall feasibility requirement study in 5. The third and fourth bullets are redundant.

Recommendation #9: The Recommendation lists seven specific "features" that may currently be used to overcome vulnerabilities in wireless communication. This list is in no way comprehensive and is limited in relevance by the application of the ID system and its design. It is random and short-sighted to list some concepts and technologies that must be evaluated while ignoring others. Further, all security risks in ID management systems should be identified and mitigated *before* implementing an ID system. Those listed here, which, contrary to the Recommendation's not to focus on RFID alone, highlight RFID-related solutions, should be evaluated among all other security risks in all other types of ID systems, and mitigated with technologies appropriate to the risk. Finally, and illustrating the problem with such lists, it is equally important to direct attention to the physical security of the card in ID systems that may be relied upon when readers do not work.

Finally, the Recommendations do not contain a technically accurate description of RFID. The never-seen-before language from page 15 should read: "Radio Frequency Identification (RFID) is an electronic system utilized to identify or track documents or items. In an RFID identification document, a small memory-storage chip (tag) or a secure integrated circuit with memory and encryption is embedded. When the document comes within the range of a receiver/transmitter known as an RFID reader (or emitter), the reader will send out radio waves or magnetic or inductively coupled energy to detect tags and read their data.

-- Respectfully submitted, June 6, 2008

Sincerely,



Roxanne Gould
Senior Vice President, State Government Affairs
AeA (American Electronics Association)
1415 L Street Ste 1260
Sacramento, CA 95814
916.443.9059 x101

Appendices

APPENDIX C

SAM FEASIBILITY STUDY

4920 PURPOSE

(Revised 09/02)

The feasibility study represents the first opportunity for agency management to assess the full implications of a proposed information technology project. The feasibility study is also the means of linking a specific information technology project to the agency's strategic business plans and information technology plans, and to ensure that the proposed project makes the best use of the agency's information technology infrastructure. The purposes of the feasibility study are to:

1. Determine whether there is a business case for a proposed project, i.e., whether the expenditure of public resources on the project is justified in terms of the project's:
 - a. Being responsive to a clearly-defined, program-related problem or opportunity;
 - b. Being the best of the possible alternatives;
 - c. Being within the technical and managerial capabilities of the agency; and
 - d. Having benefits over the life of the application that exceed development and operations costs. Project benefits typically include reduced program costs, avoidance of future program cost increases, increased program revenues, or provision of program services that can be provided only through the use of information technology.
2. Provide a means for achieving agreement between agency executive management, program management, and project management as to:
 - a. The nature, benefits, schedule, and costs of a proposed project; and

- b. Their respective management responsibilities over the course of the project.
3. Provide executive branch control agencies and the Legislature with sufficient information to assess the merits of the proposed project and determine the nature and extent of project oversight requirements.

4921 FEASIBILITY STUDY BASIC POLICY

(Revised 12/04)

A feasibility study must be conducted prior to the encumbrance or expenditure of funds on any information technology project. For most projects, the feasibility study must be conducted in conformance with SAM Sections 4922 through 4927. The only exception to this requirement is the acquisition of desktop and mobile computing commodities under the Desktop and Mobile Computing Policy. (See SAM Section 4989.) In addition, a Feasibility Study Report (FSR), which documents the feasibility study, must be approved prior to the encumbrance or expenditure of funds, including the use of staff resources, on any information technology project beyond the feasibility study stage. For most projects, the FSR must be prepared in accordance with SAM Section 4928. For projects that have been delegated to the agency director and whose costs fall below a specified level, the feasibility study may be documented by means of a Project Summary Package. See SAM Section 4930 and SIMM Section 20.

The FSR must be reviewed and approved in accordance with the general requirements of SAM Sections 4819.3-4819.42 (State Information Management Authority and Responsibility), as well as the specific requirements of Sections 4926-4930.1. See SIMM Section 20 for FSR Preparation Instructions.

4922 FEASIBILITY STUDY SCOPE

(Revised 5/94)

The scope of the feasibility study must be commensurate with the nature, complexity, risk, and expected cost of the proposed use of information technology.

The study must provide sufficient information to assure agency program management that the proposed response meets program requirements. The study also must provide sufficient information to allow agency executive management to make a sound decision as to the merits of the proposed response as an investment of public resources.

Appendices

4923 FEASIBILITY STUDY PARTICIPATION

(New 3/87)

The feasibility study must be based on an understanding of the needs, priorities, and capabilities of: (1) the users of the information that is to be provided; and (2) the agency unit or program that will have operational responsibility for the information technology application. Representatives of program management and staff must participate in the feasibility study process.

4924 FEASIBILITY STUDY DOCUMENTATION

(Revised 09/02)

The SAM Section 4928 and instructions and guidelines published by Finance (see SIMM Section 20) specify the content of the FSR, which must provide a complete summary of the results of the feasibility study. In addition to the FSR, the agency must maintain sufficient documentation of each study to ensure that project participants, agency management, and control agency personnel can resolve any questions that arise with respect to the intent, justification, nature, and scope of the project.

4925 CONSISTENCY WITH AGENCY INFORMATION MANAGEMENT STRATEGY

(Revised 5/94)

Each proposed project must be consistent with the agency's overall strategy for the use of information technology, as expressed in its current Agency Information Management Strategy. See SAM Sections 4900.2-4900.6.

4927 FEASIBILITY STUDY PROCESS

(Revised 5/94)

Each agency must follow a systematic, analytical process for evaluating and documenting the feasibility of information technology projects, as defined in SAM Section 4819.2. This process must include:

1. Developing an understanding of a problem (or opportunity) in terms of its effect on the agency's mission and programs;

2. Developing an understanding of the organizational, managerial, and technical environment within which a response to the problem or opportunity will be implemented;
3. Establishing programmatic and administrative objectives against which possible responses will be evaluated;
4. Preparing concise functional requirements of an acceptable response;
5. Identifying and evaluating possible alternative responses with respect to the established objectives;
6. Preparing an economic analysis for each alternative that meets the established objectives and functional requirements;
7. Selecting the alternative that is the best response to the problem or opportunity;
8. Preparing a management plan for implementation of the proposed response; and
9. Documenting the results of the study in the form of a Feasibility Study Report (FSR), as specified in SAM Section 4928.

4928 FEASIBILITY STUDY REPORT

(Revised 6/03)

The FSR must provide an accurate summary of the results of the feasibility study. As with the study itself, the scope of the FSR must be commensurate with the scope and complexity of the problem or opportunity being addressed. Enough technical detail must be included in the FSR to show that the proposed response to the problem or opportunity is workable and realistic. The FSR must provide a basis for understanding and agreement among project management, executive management and program management, as well as satisfy the information requirements of state-level control agencies.

The FSR must be submitted to Finance and to the Office of the Legislative Analyst. In addition, the FSR must be submitted to the Department of General Services when the contract total exceeds the agency's delegated purchasing authority threshold. FSRs must be submitted in a format specified by Finance and signed by the agency director or his/her designee. Finance

Appendices

publishes detailed instructions and guidelines for agencies' use in preparing FSRs. A copy of the instructions, guidelines, and required forms is available in SIMM Section 20. The instructions and guidelines specify the MINIMUM amount of information necessary for Finance's approval of the FSR.

The FSR must provide a complete summary of the results of the feasibility study and establish the business case for investment of state resources in a project by setting out the reasons for undertaking the project and analyzing its costs and benefits. Documentation provided by the agency must contain at least the following information:

1. A description of the business problem or opportunity the project is intended to address.
2. The project objectives, i.e., the significant results that must be achieved for an alternative to be an effective response to the problem or opportunity being addressed.
3. A thorough description of the selected alternative, including the hardware, software and personnel that will be used.
4. A discussion and economic analysis of each of the alternatives considered in the feasibility study that meets the established objectives and functional requirements, and the reasons for rejecting the alternatives that were not selected.
5. A complete description of the information technology capabilities and the conditions that must exist in order to satisfy each defined objective.
6. An economic analysis of the life cycle costs and benefits of the project and the costs and benefits of the current method of operation during the life cycle of the project.
7. The source of funding for the project.
8. A detailed project schedule showing key milestones during the project's life.

A Project Summary Package (SAM Section 4930) must be prepared and included in the FSR.

Appendices

The agency must maintain sufficient documentation of each study to ensure that project participants, agency management, and control agency personnel can resolve any questions about the intent, justification, nature, and scope of the project.

Appendices

APPENDIX D

PRIVACY PROVISIONS FROM THE E-GOVERNMENT ACT OF 2002

E-Government Act of 2002
Pub. L. No. 107-347, Dec. 17, 2002

SEC. 208. PRIVACY PROVISIONS.

A. PURPOSE. — The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

B. PRIVACY IMPACT ASSESSMENTS.—

1. RESPONSIBILITIES OF AGENCIES.—

- a. IN GENERAL.—An agency shall take actions described under subparagraph (b) before—
 - i. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
 - ii. initiating a new collection of information that—
 - 1. will be collected, maintained, or disseminated using information technology; and
 - 2. includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.
- b. AGENCY ACTIVITIES. —To the extent required under subparagraph (a), each agency shall—
 - i. conduct a privacy impact assessment;

Appendices

- ii. ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
 - iii. if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.
- c. SENSITIVE INFORMATION. —Subparagraph (b)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.
- d. COPY TO DIRECTOR. —Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

2. CONTENTS OF A PRIVACY IMPACT ASSESSMENT. —

- a. IN GENERAL. —The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.
- b. GUIDANCE. — The guidance shall—
- i. ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
 - ii. require that a privacy impact assessment address—
 - 1. what information is to be collected;
 - 2. why the information is being collected;
 - 3. the intended use of the agency of the information;
 - 4. with whom the information will be shared;
 - 5. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
 - 6. how the information will be secured; and

Appendices

7. whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the ' Privacy Act').

3. RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

- a. develop policies and guidelines for agencies on the conduct of privacy impact assessments;
- b. oversee the implementation of the privacy impact assessment process throughout the Government; and
- c. require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

C. PRIVACY PROTECTIONS ON AGENCY WEBSITES. —

1. PRIVACY POLICIES ON WEBSITES. —

- a. GUIDELINES FOR NOTICES. —The Director shall develop guidance for privacy notices on agency websites used by the public.
- b. CONTENTS. —The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—
 - i. what information is to be collected;
 - ii. why the information is being collected;
 - iii. the intended use of the agency of the information;
 - iv. with whom the information will be shared;
 - v. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
 - vi. how the information will be secured; and
 - vii. the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the ' Privacy Act'), and other laws relevant to the protection of the privacy of an individual.

Appendices

2. PRIVACY POLICIES IN MACHINE-READABLE FORMATS. — The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

D. DEFINITION. —In this section, the term 'identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Appendices

APPENDIX E

OFFICE OF MANAGEMENT AND BUDGET E-GOVERNMENT ACT SECTION 208 IMPLEMENTATION GUIDANCE

I. General

A. *Requirements.* Agencies are required to:

1. conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available (see Section II of this Guidance),
2. post privacy policies on agency websites used by the public (see Section III),
3. translate privacy policies into a standardized machine-readable format (see Section IV), and
4. report annually to OMB on compliance with section 208 of the E-Government Act of 2002 (see Section VII).

B. *Application.* This guidance applies to:

1. all executive branch departments and agencies (“agencies”) and their contractors that use information technology or that operate websites for purposes of interacting with the public;
2. relevant cross-agency initiatives, including those that further electronic government.

C. *Modifications to Current Guidance.* Where indicated, this Memorandum modifies the following three memoranda, which are replaced by this guidance (see summary of modifications at Attachment D):

1. Memorandum 99-05 (January 7, 1999), directing agencies to examine their procedures for ensuring the privacy of personal information in federal records and to designate a senior official to assume primary responsibility for privacy policy;
2. Memorandum 99-18 (June 2, 1999), concerning posting privacy policies on major entry points to government web sites as well as on any

web page collecting substantial personal information from the public;
and

3. Memorandum 00-13 (June 22, 2000), concerning (i) the use of tracking technologies such as persistent cookies and (ii) parental consent consistent with the Children's Online Privacy Protection Act ("COPPA").

II. Privacy Impact Assessment

A. *Definitions.*

1. *Individual* - means a citizen of the United States or an alien lawfully admitted for permanent residence.
2. *Information in identifiable form*- is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).
3. *Information technology (IT)* - means, as defined in the Clinger-Cohen Act, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
4. *Major information system* - embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.
5. *National Security Systems* - means, as defined in the Clinger-Cohen Act⁴, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) crypto logic activities related to national security, (c) command and

Appendices

control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.

6. *Privacy Impact Assessment (PIA)*- is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
7. *Privacy policy in standardized machine-readable format*- means a statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.

B. *When to conduct a PIA:*

1. *The E-Government Act requires agencies to conduct a PIA before:*
 - a. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
 - b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).
2. *In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:*
 - a. Conversions - when converting paper-based records to electronic systems;
 - b. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Appendices

- c. Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
 - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
- d. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
 - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
- e. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- f. Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- g. New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
 - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define

Appendices

requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.

- h. Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
 - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
 - i. Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)
3. *No PLA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PLA, or where privacy issues are unchanged, as in the following circumstances:*
- a. for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public (this includes government personnel and government contractors and consultants);
 - b. for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or obtaining additional information;

Appendices

- c. for national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act);
 - d. when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act (see 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide privacy protection for matched information;
 - e. when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act of 2002;
 - f. if agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form;
 - g. for minor changes to a system or collection that do not create new privacy risks.
4. *Update of PIAs:* Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

C. *Conducting a PIA.*

1. *Content.*

- a. PIAs must analyze and describe:
 - i. what information is to be collected (e.g., nature and source);
 - ii. why the information is being collected (e.g., to determine eligibility);
 - iii. intended use of the information (e.g., to verify existing data);

Appendices

- iv. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
 - v. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
 - vi. how the information will be secured (e.g., administrative and technological controls); and
 - vii. whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.
 - b. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
- 2. Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection:
 - a. *Specificity*. The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.
 - i. *IT development stage*. PIAs conducted at this stage:
 - 1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
 - 2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;

3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.
 - ii. *Major information systems.* PIAs conducted for these systems should reflect more extensive analyses of:
 1. the consequences of collection and flow of information,
 2. the alternatives to collection and handling as designed,
 3. the appropriate measures to mitigate risks identified for each alternative and,
 4. the rationale for the final design choice or business process.
 - iii. *Routine database systems.* Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.
 - b. *Information life cycle analysis/collaboration.* Agencies must consider the information “life cycle” (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals’ privacy. To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.
3. *Review and publication.*
 - a. Agencies must ensure that:
 - i. the PIA document and, if prepared, summary are approved by a “reviewing official” (the agency CIO or other agency head designee, who is other than the

Appendices

official procuring the system or the official who conducts the PIA);

- ii. for each covered IT system for which 2005 funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300); and
- iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).
 - 1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).
 - 2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

D. *Relationship to requirements under the Paperwork Reduction Act (PRA).*

- 1. Joint Information Collection Request (ICR) and PIA. Agencies undertaking new electronic information collections may conduct and submit the PIA to OMB, and make it publicly available, as part of the SF83 Supporting Statement (the request to OMB to approve a new agency information collection).

2. If Agencies submit a Joint ICR and PIA:
 - a. All elements of the PIA must be addressed and identifiable within the structure of the Supporting Statement to the ICR, including:
 - i. a description of the information to be collected in the response to Item 1 of the Supporting Statement;
 - ii. a description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement;
 - iii. a statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement;
 - iv. a discussion in item 10 of the Supporting Statement of:
 1. whether individuals are informed that providing the information is mandatory or voluntary
 2. opportunities to consent, if any, to sharing and submission of information;
 3. how the information will be secured; and
 4. whether a system of records is being created under the Privacy Act).
 - b. For additional information on the requirements of an ICR, please consult your agency's organization responsible for PRA compliance.
3. Agencies need not conduct a new PIA for simple renewal requests for information collections under the PRA. As determined by reference to section II.B.2. above, agencies must separately consider the need for a PIA when amending an ICR to collect information that is significantly different in character from the original collection.

E. *Relationship to requirements under the Privacy Act of 1974, 5 U.S. C. 552a.*

1. Agencies may choose to conduct a PIA when developing the System of Records (SOR) notice required by subsection (e)(4) of the Privacy Act,

Appendices

in that the PIA and SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).

2. Agencies, in addition, may make the PIA publicly available in the Federal Register along with the Privacy Act SOR notice.
3. Agencies must separately consider the need for a PIA when issuing a change to a SOR notice (e.g., a change in the type or category of record added to the system may warrant a PIA).

III. Privacy Policies on Agency Websites

- A. *Privacy Policy Clarification.* To promote clarity to the public, agencies are required to refer to their general web site notices explaining agency information handling practices as the “Privacy Policy.”
- B. *Effective Date.* Agencies are expected to implement the following changes to their websites by December 15, 2003.
- C. *Exclusions:* For purposes of web privacy policies, this guidance does not apply to:
 1. information other than “government information” as defined in OMB Circular A-130;
 2. agency intranet web sites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees);
 3. national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-government Act).
- D. *Content of Privacy Policies.*
 1. Agency Privacy Policies must comply with guidance issued in OMB Memorandum 99-18 and must now also include the following two new content areas:
 - a. *Consent to collection and sharing.* Agencies must now ensure that privacy policies:

- i. inform visitors whenever providing requested information is voluntary;
 - ii. inform visitors how to grant consent for use of voluntarily-provided information; and
 - iii. inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
 - b. *Rights under the Privacy Act or other privacy laws.* Agencies must now also notify web-site visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (such as the Health Insurance Portability and Accountability Act of 1996, the IRS Restructuring and Reform Act of 1998, or the Family Education Rights and Privacy Act):
 - i. in the body of the web privacy policy;
 - ii. via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or
 - iii. via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).
2. Agency Privacy Policies must continue to address the following, modified, requirements:
- a. Nature, purpose, use and sharing of information collected. Agencies should follow existing policies (issued in OMB Memorandum 99-18) concerning notice of the nature, purpose, use and sharing of information collected via the Internet, as modified below:
 - i. *Privacy Act information.* When agencies collect information subject to the Privacy Act, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier

Appendices

in a Privacy Act system of records and provide a Privacy Act Statement either:

1. at the point of collection, or
 2. via link to the agency's general Privacy Policy.
- ii. *"Privacy Act Statements."* Privacy Act Statements must notify users of the authority for and purpose and use of the collection of information subject to the Privacy Act, whether providing the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.
 - iii. *Automatically Collected Information (site management data).* Agency Privacy Policies must specify what information the agency collects automatically (i.e., user's IP address, location, and time of visit) and identify the use for which it is collected (i.e., site management or security purposes).
 - iv. *Interaction with children:* Agencies that provide content to children under 13 and that collect personally identifiable information from these visitors should incorporate the requirements of the Children's Online Privacy Protection Act ("COPPA") into their Privacy Policies (see Attachment C).
 - v. *Tracking and customization activities.* Agencies are directed to adhere to the following modifications to OMB Memorandum 00-13 and the OMB follow-up guidance letter dated September 5, 2000:
 1. *Tracking technology prohibitions:*
 - a. agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below;
 - b. agency heads may approve, or may authorize the heads of sub-agencies or

Appendices

senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's must post clear notice in the agency's privacy policy of:

- the nature of the information collected;
 - the purpose and use for the information;
 - whether and to whom the information will be disclosed; and
 - the privacy safeguards applied to the information collected.
- c. agencies must report the use of persistent tracking technologies as authorized for use by subsection b. above (see section VII).

2. *The following technologies are not prohibited:*

- a. Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
- b. Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see v.1.b above) and where the following is posted in the Agency's Privacy Policy:
 - the purpose of the tracking (i.e., customization of the site);

Appendices

- that accepting the customizing feature is voluntary;
 - that declining the feature still permits the individual to use the site; and
 - the privacy safeguards in place for handling the information collected.
 - c. Agency use of password access to information that does not involve “persistent cookies” or similar technology.
- vi. *Law enforcement and homeland security sharing:*
Consistent with current practice, Internet privacy policies may reflect that collected information may be shared and protected as necessary for authorized law enforcement, homeland security and national security activities.
- b. *Security of the information.* Agencies should continue to comply with existing requirements for computer security in administering their websites and post the following information in their Privacy Policy:
 - i. in clear language, information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and
 - ii. in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)

- E. *Placement of notices.* Agencies should continue to follow the policy identified in OMB Memorandum 99-18 regarding the posting of privacy policies on their websites. Specifically, agencies must post (or link to) privacy policies at:
 - 1. their principal web site;
 - 2. any known, major entry points to their sites;
 - 3. any web page that collects substantial information in identifiable form.
- F. *Clarity of notices.* Consistent with OMB Memorandum 99-18, privacy policies must be:
 - 1. clearly labeled and easily accessed;
 - 2. written in plain language; and
 - 3. made clear and easy to understand, whether by integrating all information and statements into a single posting, by layering a short “highlights” notice linked to full explanation, or by other means the agency determines is effective.

IV. Privacy Policies in Machine-Readable Formats

A. *Actions.*

- 1. Agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make an informed choice about whether to conduct business with that site.
- 2. OMB encourages agencies to adopt other privacy protective tools that become available as the technology advances.

- B. *Reporting Requirement.* Agencies must develop a timetable for translating their privacy policies into a standardized machine-readable format. The timetable must include achievable milestones that show the agency’s progress toward implementation over the next year. Agencies must include this timetable in their reports to OMB (see Section VII).

V. Privacy Policies Incorporated by this Guidance

In addition to the particular actions discussed above, this guidance reiterates general directives from previous OMB Memoranda regarding the privacy of personal

Appendices

information in federal records and collected on federal web sites. Specifically, existing policies continue to require that agencies:

- A. assure that their uses of new information technologies sustain, and do not erode, the protections provided in all statutes relating to agency use, collection, and disclosure of personal information;
- B. assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- C. evaluate legislative proposals involving collection, use and disclosure of personal information by the federal government for consistency with the Privacy Act of 1974;
- D. evaluate legislative proposals involving the collection, use and disclosure of personal information by any entity, public or private, for consistency with the Privacy Principles;
- E. ensure full adherence with stated privacy policies.

VI. Agency Privacy Activities/Designation of Responsible Official

Because of the capability of information technology to capture and disseminate information in an instant, all federal employees and contractors must remain mindful of privacy and their obligation to protect information in identifiable form. In addition, implementing the privacy provisions of the E-Government Act requires the cooperation and coordination of privacy, security, FOIA/Privacy Act and project officers located in disparate organizations within agencies. Clear leadership and authority are essential.

Accordingly, this guidance builds on policy introduced in Memorandum 99-05 in the following ways:

- A. Agencies must:
 - 1. inform and educate employees and contractors of their responsibility for protecting information in identifiable form;
 - 2. identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies.

Appendices

3. designate an appropriate senior official or officials (e.g., CIO, Assistant Secretary) to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies. The designated official(s) shall coordinate implementation of OMB web and privacy policy and guidance.
 4. designate an appropriate official (or officials, as appropriate) to serve as the "reviewing official(s)" for agency PIAs.
- B. OMB leads a committee of key officials involved in privacy that reviewed and helped shape this guidance and that will review and help shape any follow-on privacy and web-privacy-related guidance. In addition, as part of overseeing agencies' implementation of section 208, OMB will rely on the CIO Council to collect information on agencies' initial experience in preparing PIAs, to share experiences, ideas, and promising practices as well as identify any needed revisions to OMB's guidance on PIAs.

VII. Reporting Requirements

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report. The first reports are due to OMB by December 15, 2003. All agencies that use information technology systems and conduct electronic information collection activities must complete a report on compliance with this guidance, whether or not they submit budgets to OMB.

Reports must address the following four elements:

- A. *Information technology systems or information collections for which PIAs were conducted.* Include the mechanism by which the PIA was made publicly available (website, Federal Register, other), whether the PIA was made publicly available in full, summary form or not at all (if in summary form or not at all, explain), and, if made available in conjunction with an ICR or SOR, the publication date.
- B. *Persistent tracking technology uses.* If persistent tracking technology is authorized, include the need that compels use of the technology, the safeguards instituted to protect the information collected, the agency official approving use of the tracking technology, and the actual privacy policy notification of such use.

Appendices

- C. *Agency achievement of goals for machine readability*: Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.
- D. *Contact information*. Include the individual(s) (name and title) appointed by the head of the Executive Department or agency to serve as the agency's principal contact(s) for information technology/web matters and the individual (name and title) primarily responsible for privacy policies.

APPENDIX F

PUBLIC PARTICIPATION PROVISIONS OF THE ADMINISTRATIVE PROCEDURES ACT

GOVERNMENT CODE SECTIONS 11346-11348

§ 11346. Purpose and applicability of article; Subsequent legislation

(a) It is the purpose of this chapter to establish basic minimum procedural requirements for the adoption, amendment, or repeal of administrative regulations. Except as provided in Section 11346.1, the provisions of this chapter are applicable to the exercise of any quasi-legislative power conferred by any statute heretofore or hereafter enacted, but nothing in this chapter repeals or diminishes additional requirements imposed by any statute. This chapter shall not be superseded or modified by any subsequent legislation except to the extent that the legislation shall do so expressly.

(b) An agency that is considering adopting, amending, or repealing a regulation may consult with interested persons before initiating regulatory action pursuant to this article.

§ 11346.1. Emergency regulations and orders of repeal

(a)

(1) The adoption, amendment, or repeal of an emergency regulation is not subject to any provision of this article or Article 6 (commencing with Section 11349), except this section and Sections 11349.5 and 11349.6.

(2) At least five working days before submitting an emergency regulation to the office, the adopting agency shall, except as provided in paragraph (3), send a notice of the proposed emergency action to every person who has filed a request for notice of regulatory action with the agency. The notice shall include both of the following:

(A) The specific language proposed to be adopted.

(B) The finding of emergency required by subdivision (b).

(3) An agency is not required to provide notice pursuant to paragraph (2) if the emergency situation clearly poses such an immediate, serious harm that delaying action to allow public comment would be inconsistent with the public interest.

(b)

Appendices

(1) Except as provided in subdivision (c), if a state agency makes a finding that the adoption of a regulation or order of repeal is necessary to address an emergency, the regulation or order of repeal may be adopted as an emergency regulation or order of repeal.

(2) Any finding of an emergency shall include a written statement that contains the information required by paragraphs (2) to (6), inclusive, of subdivision (a) of Section 11346.5 and a description of the specific facts demonstrating the existence of an emergency and the need for immediate action, and demonstrating, by substantial evidence, the need for the proposed regulation to effectuate the statute being implemented, interpreted, or made specific and to address only the demonstrated emergency. The finding of emergency shall also identify each technical, theoretical, and empirical study, report, or similar document, if any, upon which the agency relies. The enactment of an urgency statute shall not, in and of itself, constitute a need for immediate action.

A finding of emergency based only upon expediency, convenience, best interest, general public need, or speculation, shall not be adequate to demonstrate the existence of an emergency. If the situation identified in the finding of emergency existed and was known by the agency adopting the emergency regulation in sufficient time to have been addressed through nonemergency regulations adopted in accordance with the provisions of Article 5 (commencing with Section 11346), the finding of emergency shall include facts explaining the failure to address the situation through nonemergency regulations.

(3) The statement and the regulation or order of repeal shall be filed immediately with the office.

(c) Notwithstanding any other provision of law, no emergency regulation that is a building standard shall be filed, nor shall the building standard be effective, unless the building standard is submitted to the California Building Standards Commission, and is approved and filed pursuant to Sections 18937 and 18938 of the Health and Safety Code.

(d) The emergency regulation or order of repeal shall become effective upon filing or upon any later date specified by the state agency in a written instrument filed with, or as a part of, the regulation or order of repeal.

(e) No regulation, amendment, or order of repeal initially adopted as an emergency regulatory action shall remain in effect more than 180 days unless the adopting agency has complied with Sections 11346.2 to 11347.3, inclusive, either before adopting an emergency regulation or within the 180-day period. The adopting agency, prior to the expiration of the 180-day period, shall transmit to the office for filing with the Secretary of State the adopted regulation, amendment, or order of repeal, the rulemaking file, and a certification that Sections 11346.2 to 11347.3, inclusive, were complied with either before the emergency regulation was adopted or within the 180-day period.

(f) If an emergency amendment or order of repeal is filed and the adopting agency fails to comply with subdivision (e), the regulation as it existed prior to the emergency amendment or

order of repeal shall thereupon become effective and after notice to the adopting agency by the office shall be reprinted in the California Code of Regulations.

(g) If a regulation is originally adopted and filed as an emergency and the adopting agency fails to comply with subdivision (e), this failure shall constitute a repeal of the regulation and after notice to the adopting agency by the office, shall be deleted.

(h) The office may approve not more than two readoptions, each for a period not to exceed 90 days, of an emergency regulation that is the same as or substantially equivalent to an emergency regulation previously adopted by that agency. Readoption shall be permitted only if the agency has made substantial progress and proceeded with diligence to comply with subdivision (e).

§ 11346.2. Availability to public of copy of proposed regulation; Initial statement of reasons for proposed action

Every agency subject to this chapter shall prepare, submit to the office with the notice of the proposed action as described in Section 11346.5, and make available to the public upon request, all of the following:

(a) A copy of the express terms of the proposed regulation.

(1) The agency shall draft the regulation in plain, straightforward language, avoiding technical terms as much as possible, and using a coherent and easily readable style. The agency shall draft the regulation in plain English.

(2) The agency shall include a notation following the express terms of each California Code of Regulations section, listing the specific statutes or other provisions of law authorizing the adoption of the regulation and listing the specific statutes or other provisions of law being implemented, interpreted, or made specific by that section in the California Code of Regulations.

(3) The agency shall use underline or italics to indicate additions to, and strikeout to indicate deletions from, the California Code of Regulations.

(b) An initial statement of reasons for proposing the adoption, amendment, or repeal of a regulation. This statement of reasons shall include, but not be limited to, all of the following:

(1) A statement of the specific purpose of each adoption, amendment, or repeal and the rationale for the determination by the agency that each adoption, amendment, or repeal is reasonably necessary to carry out the purpose for which it is proposed. Where the adoption or amendment of a regulation would mandate the use of specific technologies or equipment, a statement of the reasons why the agency believes these mandates or prescriptive standards are required.

Appendices

(2) An identification of each technical, theoretical, and empirical study, report, or similar document, if any, upon which the agency relies in proposing the adoption, amendment, or repeal of a regulation.

(3)

(A) A description of reasonable alternatives to the regulation and the agency's reasons for rejecting those alternatives. In the case of a regulation that would mandate the use of specific technologies or equipment or prescribe specific actions or procedures, the imposition of performance standards shall be considered as an alternative.

(B) A description of reasonable alternatives to the regulation that would lessen any adverse impact on small business and the agency's reasons for rejecting those alternatives.

(C) Notwithstanding subparagraph (A) or (B), an agency is not required to artificially construct alternatives, describe unreasonable alternatives, or justify why it has not described alternatives.

(4) Facts, evidence, documents, testimony, or other evidence on which the agency relies to support an initial determination that the action will not have a significant adverse economic impact on business.

(5) A department, board, or commission within the Environmental Protection Agency, the Resources Agency, or the Office of the State Fire Marshal shall describe its efforts, in connection with a proposed rulemaking action, to avoid unnecessary duplication or conflicts with federal regulations contained in the Code of Federal Regulations addressing the same issues. These agencies may adopt regulations different from federal regulations contained in the Code of Federal Regulations addressing the same issues upon a finding of one or more of the following justifications:

(A) The differing state regulations are authorized by law.

(B) The cost of differing state regulations is justified by the benefit to human health, public safety, public welfare, or the environment.

(c) A state agency that adopts or amends a regulation mandated by federal law or regulations, the provisions of which are identical to a previously adopted or amended federal regulation, shall be deemed to have complied with subdivision (b) if a statement to the effect that a federally mandated regulation or amendment to a regulation is being proposed, together with a citation to where an explanation of the provisions of the regulation can be found, is included in the notice of proposed adoption or amendment prepared pursuant to Section 11346.5. However, the agency shall comply fully with this chapter with respect to any provisions in the regulation that the agency proposes to adopt or amend that are different from the corresponding provisions of the federal regulation.

§ 11346.3. Assessment of potential for adverse economic impact on businesses and individuals

(a) State agencies proposing to adopt, amend, or repeal any administrative regulation shall assess the potential for adverse economic impact on California business enterprises and individuals, avoiding the imposition of unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements. For purposes of this subdivision, assessing the potential for adverse economic impact shall require agencies, when proposing to adopt, amend, or repeal a regulation, to adhere to the following requirements, to the extent that these requirements do not conflict with other state or federal laws:

(1) The proposed adoption, amendment, or repeal of a regulation shall be based on adequate information concerning the need for, and consequences of, proposed governmental action.

(2) The state agency, prior to submitting a proposal to adopt, amend, or repeal a regulation to the office, shall consider the proposal's impact on business, with consideration of industries affected including the ability of California businesses to compete with businesses in other states. For purposes of evaluating the impact on the ability of California businesses to compete with businesses in other states, an agency shall consider, but not be limited to, information supplied by interested parties.

It is not the intent of this section to impose additional criteria on agencies, above that which exists in current law, in assessing adverse economic impact on California business enterprises, but only to assure that the assessment is made early in the process of initiation and development of a proposed adoption, amendment, or repeal of a regulation.

(b)

(1) All state agencies proposing to adopt, amend, or repeal any administrative regulations shall assess whether and to what extent it will affect the following:

(A) The creation or elimination of jobs within the State of California.

(B) The creation of new businesses or the elimination of existing businesses within the State of California.

(C) The expansion of businesses currently doing business within the State of California.

(2) This subdivision does not apply to the University of California, the Hastings College of the Law, or the Fair Political Practices Commission.

(3) Information required from state agencies for the purpose of completing the assessment may come from existing state publications.

(c) No administrative regulation adopted on or after January 1, 1993, that requires a report shall apply to businesses, unless the state agency adopting the regulation makes a finding that it

Appendices

is necessary for the health, safety, or welfare of the people of the state that the regulation apply to businesses.

§ 11346.4. Notice of proposed action

(a) At least 45 days prior to the hearing and close of the public comment period on the adoption, amendment, or repeal of a regulation, notice of the proposed action shall be:

(1) Mailed to every person who has filed a request for notice of regulatory actions with the state agency. Each state agency shall give a person filing a request for notice of regulatory actions the option of being notified of all proposed regulatory actions or being notified of regulatory actions concerning one or more particular programs of the state agency.

(2) In cases in which the state agency is within a state department, mailed or delivered to the director of the department.

(3) Mailed to a representative number of small business enterprises or their representatives that are likely to be affected by the proposed action. "Representative" for the purposes of this paragraph includes, but is not limited to, a trade association, industry association, professional association, or any other business group or association of any kind that represents a business enterprise or employees of a business enterprise.

(4) When appropriate in the judgment of the state agency, mailed to any person or group of persons whom the agency believes to be interested in the proposed action and published in the form and manner as the state agency shall prescribe.

(5) Published in the California Regulatory Notice Register as prepared by the office for each state agency's notice of regulatory action.

(6) Posted on the state agency's website if the agency has a website.

(b) The effective period of a notice issued pursuant to this section shall not exceed one year from the date thereof. If the adoption, amendment, or repeal of a regulation proposed in the notice is not completed and transmitted to the office within the period of one year, a notice of the proposed action shall again be issued pursuant to this article.

(c) Once the adoption, amendment, or repeal is completed and approved by the office, no further adoption, amendment, or repeal to the noticed regulation shall be made without subsequent notice being given.

(d) The office may refuse to publish a notice submitted to it if the agency has failed to comply with this article.

(e) The office shall make the California Regulatory Notice Register available to the public and state agencies at a nominal cost that is consistent with a policy of encouraging the widest possible notice distribution to interested persons.

(f) Where the form or manner of notice is prescribed by statute in any particular case, in addition to filing and mailing notice as required by this section, the notice shall be published, posted, mailed, filed, or otherwise publicized as prescribed by that statute. The failure to mail notice to any person as provided in this section shall not invalidate any action taken by a state agency pursuant to this article.

§ 11346.45. Increased public participation

(a) In order to increase public participation and improve the quality of regulations, state agencies proposing to adopt regulations shall, prior to publication of the notice required by Section 11346.5, involve parties who would be subject to the proposed regulations in public discussions regarding those proposed regulations, when the proposed regulations involve complex proposals or a large number of proposals that cannot easily be reviewed during the comment period.

(b) This section does not apply to a state agency in any instance where that state agency is required to implement federal law and regulations for which there is little or no discretion on the part of the state to vary.

(c) If the agency does not or cannot comply with the provisions of subdivision (a), it shall state the reasons for noncompliance with reasonable specificity in the rulemaking record.

(d) The provisions of this section shall not be subject to judicial review or to the provisions of Section 11349.1.

§ 11346.5. Contents of notice of proposed adoption, amendment, or repeal of regulation

(a) The notice of proposed adoption, amendment, or repeal of a regulation shall include the following:

(1) A statement of the time, place, and nature of proceedings for adoption, amendment, or repeal of the regulation.

(2) Reference to the authority under which the regulation is proposed and a reference to the particular code sections or other provisions of law that are being implemented, interpreted, or made specific.

(3) An informative digest drafted in plain English in a format similar to the Legislative Counsel's digest on legislative bills. The informative digest shall include the following:

(A) A concise and clear summary of existing laws and regulations, if any, related directly to the proposed action and of the effect of the proposed action.

Appendices

(B) If the proposed action differs substantially from an existing comparable federal regulation or statute, a brief description of the significant differences and the full citation of the federal regulations or statutes.

(C) A policy statement overview explaining the broad objectives of the regulation and, if appropriate, the specific objectives.

(4) Any other matters as are prescribed by statute applicable to the specific state agency or to any specific regulation or class of regulations.

(5) A determination as to whether the regulation imposes a mandate on local agencies or school districts and, if so, whether the mandate requires state reimbursement pursuant to Part 7 (commencing with Section 17500) of Division 4.

(6) An estimate, prepared in accordance with instructions adopted by the Department of Finance, of the cost or savings to any state agency, the cost to any local agency or school district that is required to be reimbursed under Part 7 (commencing with Section 17500) of Division 4, other nondiscretionary cost or savings imposed on local agencies, and the cost or savings in federal funding to the state.

For purposes of this paragraph, "cost or savings" means additional costs or savings, both direct and indirect, that a public agency necessarily incurs in reasonable compliance with regulations.

(7) If a state agency, in proposing to adopt, amend, or repeal any administrative regulation, makes an initial determination that the action may have a significant, statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states, it shall include the following information in the notice of proposed action:

(A) Identification of the types of businesses that would be affected.

(B) A description of the projected reporting, recordkeeping, and other compliance requirements that would result from the proposed action.

(C) The following statement: "The (name of agency) has made an initial determination that the (adoption/amendment/repeal) of this regulation may have a significant, statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states. The (name of agency)(has/has not) considered proposed alternatives that would lessen any adverse economic impact on business and invites you to submit proposals. Submissions may include the following considerations:

(i) The establishment of differing compliance or reporting requirements or timetables that take into account the resources available to businesses.

(ii) Consolidation or simplification of compliance and reporting requirements for businesses.

(iii) The use of performance standards rather than prescriptive standards.

(iv) Exemption or partial exemption from the regulatory requirements for businesses."

(8) If a state agency, in adopting, amending, or repealing any administrative regulation, makes an initial determination that the action will not have a significant, statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states, it shall make a declaration to that effect in the notice of proposed action. In making this declaration, the agency shall provide in the record facts, evidence, documents, testimony, or other evidence upon which the agency relies to support its initial determination.

An agency's initial determination and declaration that a proposed adoption, amendment, or repeal of a regulation may have or will not have a significant, adverse impact on businesses, including the ability of California businesses to compete with businesses in other states, shall not be grounds for the office to refuse to publish the notice of proposed action.

(9) A description of all cost impacts, known to the agency at the time the notice of proposed action is submitted to the office, that a representative private person or business would necessarily incur in reasonable compliance with the proposed action.

If no cost impacts are known to the agency, it shall state the following:

"The agency is not aware of any cost impacts that a representative private person or business would necessarily incur in reasonable compliance with the proposed action."

(10) A statement of the results of the assessment required by subdivision (b) of Section 11346.3.

(11) The finding prescribed by subdivision (c) of Section 11346.3, if required.

(12) A statement that the action would have a significant effect on housing costs, if a state agency, in adopting, amending, or repealing any administrative regulation, makes an initial determination that the action would have that effect. In addition, the agency officer designated in paragraph (14), shall make available to the public, upon request, the agency's evaluation, if any, of the effect of the proposed regulatory action on housing costs.

(13) A statement that the adopting agency must determine that no reasonable alternative considered by the agency or that has otherwise been identified and brought to the attention of the agency would be more effective in carrying out the purpose for which the action is proposed or would be as effective and less burdensome to affected private persons than the proposed action.

(14) The name and telephone number of the agency representative and designated backup contact person to whom inquiries concerning the proposed administrative action may be directed.

Appendices

(15) The date by which comments submitted in writing must be received to present statements, arguments, or contentions in writing relating to the proposed action in order for them to be considered by the state agency before it adopts, amends, or repeals a regulation.

(16) Reference to the fact that the agency proposing the action has prepared a statement of the reasons for the proposed action, has available all the information upon which its proposal is based, and has available the express terms of the proposed action, pursuant to subdivision (b).

(17) A statement that if a public hearing is not scheduled, any interested person or his or her duly authorized representative may request, no later than 15 days prior to the close of the written comment period, a public hearing pursuant to Section 11346.8.

(18) A statement indicating that the full text of a regulation changed pursuant to Section 11346.8 will be available for at least 15 days prior to the date on which the agency adopts, amends, or repeals the resulting regulation.

(19) A statement explaining how to obtain a copy of the final statement of reasons once it has been prepared pursuant to subdivision (a) of Section 11346.9.

(20) If the agency maintains an Internet web site or other similar forum for the electronic publication or distribution of written material, a statement explaining how materials published or distributed through that forum can be accessed.

(b) The agency representative designated in paragraph (14) of subdivision (a) shall make available to the public upon request the express terms of the proposed action. The representative shall also make available to the public upon request the location of public records, including reports, documentation, and other materials, related to the proposed action. If the representative receives an inquiry regarding the proposed action that the representative cannot answer, the representative shall refer the inquiry to another person in the agency for a prompt response.

(c) This section shall not be construed in any manner that results in the invalidation of a regulation because of the alleged inadequacy of the notice content or the summary or cost estimates, or the alleged inadequacy or inaccuracy of the housing cost estimates, if there has been substantial compliance with those requirements.

§ 11346.7. Link on website

The office shall maintain a link on its website to the website maintained by the Small Business Advocate that also includes the telephone number of the Small Business Advocate.

§ 11346.8. Hearing

(a) If a public hearing is held, both oral and written statements, arguments, or contentions, shall be permitted. The agency may impose reasonable limitations on oral presentations. If a public hearing is not scheduled, the state agency shall, consistent with Section 11346.4, afford any interested person or his or her duly authorized representative, the opportunity to present statements, arguments or contentions in writing. In addition, a public hearing shall be held if, no later than 15 days prior to the close of the written comment period, an interested person or his or her duly authorized representative submits in writing to the state agency, a request to hold a public hearing. The state agency shall, to the extent practicable, provide notice of the time, date, and place of the hearing by mailing the notice to every person who has filed a request for notice thereby with the state agency. The state agency shall consider all relevant matter presented to it before adopting, amending, or repealing any regulation.

(b) In any hearing under this section, the state agency or its duly authorized representative shall have authority to administer oaths or affirmations. An agency may continue or postpone a hearing from time to time to the time and at the place as it determines. If a hearing is continued or postponed, the state agency shall provide notice to the public as to when it will be resumed or rescheduled.

(c) No state agency may adopt, amend, or repeal a regulation which has been changed from that which was originally made available to the public pursuant to Section 11346.5, unless the change is (1) nonsubstantial or solely grammatical in nature, or (2) sufficiently related to the original text that the public was adequately placed on notice that the change could result from the originally proposed regulatory action. If a sufficiently related change is made, the full text of the resulting adoption, amendment, or repeal, with the change clearly indicated, shall be made available to the public for at least 15 days before the agency adopts, amends, or repeals the resulting regulation. Any written comments received regarding the change must be responded to in the final statement of reasons required by Section 11346.9.

(d) No state agency shall add any material to the record of the rulemaking proceeding after the close of the public hearing or comment period, unless the agency complies with Section 11347.1. This subdivision does not apply to material prepared pursuant to Section 11346.9.

(e) If a comment made at a public hearing raises a new issue concerning a proposed regulation and a member of the public requests additional time to respond to the new issue before the state agency takes final action, it is the intent of the Legislature that rulemaking agencies consider granting the request for additional time if, under the circumstances, granting the request is practical and does not unduly delay action on the regulation.

Appendices

§ 11346.9. Final statements of reasons for proposing adoption or amendment of regulation; Informative digest

Every agency subject to this chapter shall do the following:

(a) Prepare and submit to the office with the adopted regulation a final statement of reasons that shall include all of the following:

(1) An update of the information contained in the initial statement of reasons. If the update identifies any data or any technical, theoretical or empirical study, report, or similar document on which the agency is relying in proposing the adoption, amendment, or repeal of a regulation that was not identified in the initial statement of reasons, or which was otherwise not identified or made available for public review prior to the close of the public comment period, the agency shall comply with Section 11347.1.

(2) A determination as to whether adoption, amendment, or repeal of the regulation imposes a mandate on local agencies or school districts. If the determination is that adoption, amendment, or repeal of the regulation would impose a local mandate, the agency shall state whether the mandate is reimbursable pursuant to Part 7 (commencing with Section 17500) of Division 4. If the agency finds that the mandate is not reimbursable, it shall state the reasons for that finding.

(3) A summary of each objection or recommendation made regarding the specific adoption, amendment, or repeal proposed, together with an explanation of how the proposed action has been changed to accommodate each objection or recommendation, or the reasons for making no change. This requirement applies only to objections or recommendations specifically directed at the agency's proposed action or to the procedures followed by the agency in proposing or adopting the action. The agency may aggregate and summarize repetitive or irrelevant comments as a group, and may respond to repetitive comments or summarily dismiss irrelevant comments as a group. For the purposes of this paragraph, a comment is "irrelevant" if it is not specifically directed at the agency's proposed action or to the procedures followed by the agency in proposing or adopting the action.

(4) A determination with supporting information that no alternative considered by the agency would be more effective in carrying out the purpose for which the regulation is proposed or would be as effective and less burdensome to affected private persons than the adopted regulation.

(5) An explanation setting forth the reasons for rejecting any proposed alternatives that would lessen the adverse economic impact on small businesses.

(b) Prepare and submit to the office with the adopted regulation an updated informative digest containing a clear and concise summary of the immediately preceding laws and regulations, if any, relating directly to the adopted, amended, or repealed regulation and the

effect of the adopted, amended, or repealed regulation. The informative digest shall be drafted in a format similar to the Legislative Counsel's Digest on legislative bills.

(c) A state agency that adopts or amends a regulation mandated by federal law or regulations, the provisions of which are identical to a previously adopted or amended federal regulation, shall be deemed to have complied with this section if a statement to the effect that a federally mandated regulation or amendment to a regulation is being proposed, together with a citation to where an explanation of the provisions of the regulation can be found, is included in the notice of proposed adoption or amendment prepared pursuant to Section 11346.5. However, the agency shall comply fully with this chapter with respect to any provisions in the regulation which the agency proposes to adopt or amend that are different from the corresponding provisions of the federal regulation.

(d) If an agency determines that a requirement of this section can be satisfied by reference to an agency statement made pursuant to Sections 11346.2 to 11346.5, inclusive, the agency may satisfy the requirement by incorporating the relevant statement by reference.

§ 11347. Decision not to proceed with proposed action

(a) If, after publication of a notice of proposed action pursuant to Section 11346.4, but before the notice of proposed action becomes ineffective pursuant to subdivision (b) of that section, an agency decides not to proceed with the proposed action, it shall deliver notice of its decision to the office for publication in the California Regulatory Notice Register.

(b) Publication of a notice under this section terminates the effect of the notice of proposed action referred to in the notice. Nothing in this section precludes an agency from proposing a new regulatory action that is similar or identical to a regulatory action that was previously the subject of a notice published under this section.

§ 11347.1. Addition to rulemaking file

(a) An agency that adds any technical, theoretical, or empirical study, report, or similar document to the rulemaking file after publication of the notice of proposed action and relies on the document in proposing the action shall make the document available as required by this section.

(b) At least 15 calendar days before the proposed action is adopted by the agency, the agency shall mail to all of the following persons a notice identifying the added document and stating the place and business hours that the document is available for public inspection:

- (1) Persons who testified at the public hearing.
- (2) Persons who submitted written comments at the public hearing.

Appendices

(3) Persons whose comments were received by the agency during the public comment period.

(4) Persons who requested notification from the agency of the availability of changes to the text of the proposed regulation.

(c) The document shall be available for public inspection at the location described in the notice for at least 15 calendar days before the proposed action is adopted by the agency.

(d) Written comments on the document or information received by the agency during the availability period shall be summarized and responded to in the final statement of reasons as provided in Section 11346.9.

(e) The rulemaking file shall contain a statement confirming that the agency complied with the requirements of this section and stating the date on which the notice was mailed.

(f) If there are no persons in categories listed in subdivision (b), then the rulemaking file shall contain a confirming statement to that effect.

§ 11347.3. File of rulemaking: Contents and availability of file

(a) Every agency shall maintain a file of each rulemaking that shall be deemed to be the record for that rulemaking proceeding. Commencing no later than the date that the notice of the proposed action is published in the California Regulatory Notice Register, and during all subsequent periods of time that the file is in the agency's possession, the agency shall make the file available to the public for inspection and copying during regular business hours.

(b) The rulemaking file shall include:

(1) Copies of any petitions received from interested persons proposing the adoption, amendment, or repeal of the regulation, and a copy of any decision provided for by subdivision (d) of Section 11340.7, which grants a petition in whole or in part.

(2) All published notices of proposed adoption, amendment, or repeal of the regulation, and an updated informative digest, the initial statement of reasons, and the final statement of reasons.

(3) The determination, together with the supporting data required by paragraph (5) of subdivision (a) of Section 11346.5.

(4) The determination, together with the supporting data required by paragraph (8) of subdivision (a) of Section 11346.5.

(5) The estimate, together with the supporting data and calculations, required by paragraph (6) of subdivision (a) of Section 11346.5.

(6) All data and other factual information, any studies or reports, and written comments submitted to the agency in connection with the adoption, amendment, or repeal of the regulation.

(7) All data and other factual information, technical, theoretical, and empirical studies or reports, if any, on which the agency is relying in the adoption, amendment, or repeal of a regulation, including any cost impact estimates as required by Section 11346.3.

(8) A transcript, recording, or minutes of any public hearing connected with the adoption, amendment, or repeal of the regulation.

(9) The date on which the agency made the full text of the proposed regulation available to the public for 15 days prior to the adoption, amendment, or repeal of the regulation, if required to do so by subdivision (c) of Section 11346.8.

(10) The text of regulations as originally proposed and the modified text of regulations, if any, that were made available to the public prior to adoption.

(11) Any other information, statement, report, or data that the agency is required by law to consider or prepare in connection with the adoption, amendment, or repeal of a regulation.

(12) An index or table of contents that identifies each item contained in the rulemaking file. The index or table of contents shall include an affidavit or a declaration under penalty of perjury in the form specified by Section 2015.5 of the Code of Civil Procedure by the agency official who has compiled the rulemaking file, specifying the date upon which the record was closed, and that the file or the copy, if submitted, is complete.

(c) Every agency shall submit to the office with the adopted regulation, the rulemaking file or a complete copy of the rulemaking file.

(d) The rulemaking file shall be made available by the agency to the public, and to the courts in connection with the review of the regulation.

(e) Upon filing a regulation with the Secretary of State pursuant to Section 11349.3, the office shall return the related rulemaking file to the agency, after which no item contained in the file shall be removed, altered, or destroyed or otherwise disposed of. The agency shall maintain the file unless it elects to transmit the file to the State Archives pursuant to subdivision (f).

(f) The agency may transmit the rulemaking file to the State Archives. The file shall include instructions that the Secretary of State shall not remove, alter, or destroy or otherwise dispose of any item contained in the file. Pursuant to Section 12223.5, the Secretary of State may designate a time for the delivery of the rulemaking file to the State Archives in consideration of document processing or storage limitations.

Appendices

§ 11348. Rulemaking records

Each agency subject to this chapter shall keep its rulemaking records on all of that agency's pending rulemaking actions, in which the notice has been published in the California Regulatory Notice Register, current and in one central location.

APPENDIX G

STATE ADMINISTRATIVE MANUAL SECTION 4841.2

INFORMATION INTEGRITY AND SECURITY

Each agency must provide for the integrity and security of its information assets by:

1. Identifying all automated files and data bases for which the agency has ownership responsibility (see SAM Section 4841.4);
2. Ensuring that responsibility for each automated file or data base is defined with respect to:
 - a. The designated owner of the information within the agency,
 - b. Custodians of information, and
 - c. Users of the information;
 - d. Ensuring that each automated file or database is identified as to its information class (see SAM Section 4841.3) in accordance with law and administrative policy;
 - e. Establishing appropriate policies and procedures for preserving the integrity and security of each automated file or data base including:
 - 1) Agreements with non-state entities, to cover, at a minimum, the following:
 - a) Appropriate levels of confidentiality for the data based on data classification (see SAM Section 4841.3);
 - b) Standards for transmission and storage of the data, if applicable;

Appendices

- c) Agreements to comply with all State policy and law regarding use of information resources and data;
 - d) Signed confidentiality statements;
 - e) Agreement to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used; and
 - f) Agreement to notify the State data owners promptly if a security incident involving the data occurs.
- 2) Identifying computing systems that allow dial-up communication or Internet access to sensitive or confidential information and information necessary for the support of agency critical applications;
- 3) Auditing usage of dial-up communications and Internet access for security violations;
- 4) Periodically changing dial-up access telephone numbers;
- 5) Responding to losses, misuse, or improper dissemination of information;
- 6) Requiring that if a data file is downloaded to a mobile device or desktop computer from another computer system, the specifications for information integrity and security which have been established for the original data file must be applied in the new environment.
- 7) Requiring encryption, or equally effective measures, for all personal, sensitive, or confidential information that is stored portable electronic storage media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers). This policy does not apply to mainframe and server tapes.

For the purpose of this policy, the terms "confidential information" and "sensitive information" are defined in SAM Sections 4841.3. For the purpose of this policy, "personal information" is defined in three categories in SAM 4841.3 as follows:

- notice-triggering information (Civil Code Section 1798.29),

- protected health information (45 C.F.R. Section 160.103), and
- electronic health information (45 C.F.R. Section 160.103).

Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the agency ISO.

3. Establishing appropriate departmental policies and procedures to protect and secure IT infrastructure, including:

- a. Technology upgrade policy, which includes, but is not limited to, operating system upgrades on servers, routers, and firewalls. The policy must address appropriate planning and testing of upgrades, in addition to departmental criteria for deciding which upgrades to apply.
- b. Security patches and security upgrade policy, which includes, but is not limited to, servers, routers, desktop computers, mobile devices, and firewalls. The policy must address application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied, and how quickly.
- c. Firewall configuration policy, which must require creation and documentation of a baseline configuration for each firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
- d. Server configuration policy, which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy must require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
- e. Server hardening policy, which must cover all servers throughout the department, not only those that fall within the jurisdiction of the department's IT area. The policy must include the process for making changes based on newly published vulnerability information as it

Appendices

becomes available. Further, the policy must address, and be consistent, with the department's policy for making security upgrades and security patches.

f. Software management and software licensing policy, which must address acquisition from reliable and safe sources, and must clearly state the department's policy about not using pirated or unlicensed software.

4. Each agency must establish policy to ensure that the use of peer-to-peer technology for any non-business purpose is prohibited. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property.

Business use of peer-to-peer technologies must be approved by the CIO and ISO.

Each state data center must carry out these responsibilities for those automated files, databases, and computer systems for which it has ownership responsibility. See SAM Sections 4841.4 and 4841.5.

Oversight responsibility at the agency level for ensuring the integrity and security of automated files, databases, and computer systems must be vested in the agency Information Security Officer.

The head of each agency is responsible for compliance with the policy in this section. See SAM Section 4841.1.